COATES-WILES TOWERS FOR CM ABELIAN VARIETIES

CHRISTOPHER M. ROWE

Abstract. The aim of this paper is to compute congruence relations on units in fields generated by adjoining torsion points of a CM abelian variety to a number field. For elliptic curves, congruence relations of the form we compute were an important ingredient in the early proofs of the Coates-Wiles theorem. In general, we compute congruence relations on exterior products of units in division fields, which more naturally fit into the framework of Rubin's generalization of Stark's conjecture.

Introduction

Let E be an elliptic curve defined over F with complex multiplication by the ring of integers of an imaginary quadratic extension K of $\mathbb{Q}$, where F is either K or $\mathbb{Q}$. In [CW77], Coates and Wiles proved that if $E(K)$ has positive rank then the Hasse-Weil L-series $L(E/F, s)$ vanishes at $s = 1$. (In Rubin's important work on Tate-Shafarevich groups, he determined bounds on Selmer groups, which yield another proof of the Coates-Wiles theorem [Rub87].)

Coates and Wiles used formal groups and Iwasawa-theoretic techniques to relate elliptic units with special values of $L(E/F, s)$. Using more classical techniques, Stark and Gupta were able to give a proof of the Coates-Wiles theorem for elliptic curves defined over $\mathbb{Q}$ [Sta83, Gup85]. The proofs utilize different techniques, but both include many of the same ideas.

Specifically, let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication (CM) by the ring of integers of an imaginary quadratic extension K of $\mathbb{Q}$ (so necessarily of class number one). Let $\mathfrak{p} = (\pi)$ be one of infinitely many suitably chosen primes of K, and K_n the field of π^n-division values of E (i.e., the finite extension of K obtained by adjoining all the π^n-torsion of E to K). Then there exists a unique prime $\mathfrak{p}_n$ of K_n lying over $\mathfrak{p}$. Fix a point $Q \in E(\mathbb{Q}) \setminus \pi E(\mathbb{Q})$ of infinite order and let L_n be the field of $\mathfrak{p}^n$-division values of Q, i.e., $L_n = K_n(\frac{1}{\mathfrak{p}^n}Q)$.

Gupta showed there exists a positive integer e such that the conductor of the field extension L_e/K_e is $\mathfrak{p}_e^2$, and then by class field theory all units of K_e congruent to $1 \bmod \mathfrak{p}_e$ are also congruent to $1 \bmod \mathfrak{p}_e^2$. Both Coates and Wiles and Gupta used a congruence relation of this form to show that $\pi | L(E/\mathbb{Q}, 1)$, and hence $L(E/\mathbb{Q}, 1)$ vanishes.

The goal of this paper is to compute conductors and congruence relations on units for CM abelian varieties paralleling the work of Gupta for CM elliptic curves. In particular, let A be an abelian variety of dimension g defined over a Galois number field

2000 *Mathematics Subject Classification.* Primary: 11G10; Primary: 11G15; Secondary: 11R27.

K with complex multiplication by the ring of integers of K (with the degree $2g$ over $\mathbb{Q}$). Furthermore let $\mathfrak{p}$ be a prime of K lying over the odd rational prime p, and assume that both p splits completely in K and A has good reduction at all primes lying over p. Then we describe congruence relations on units of K_n, the extension of K generated by the $\mathfrak{p}^n$-torsion points of A. For abelian surfaces, Grant described congruence relations on units similar to those of Gupta (see [Gra88]), but additional progress was stymied by the lack of understanding and construction of "abelian units" to parallel the theory of elliptic units. Moreover, it seems to be a difficult problem to come up with a general theory of abelian units.

Since we require that p splits completely, the field extensions K_n/K can be shown to have degree $p^{n-1}(p-1)$ and to be totally ramified at half of the primes of K lying above p and unramified at the other half (which primes ramify depends upon $\mathfrak{p}$ and the "CM type" of A). We fix a point $Q \in A(K) \setminus \mathfrak{p}A(K)$ of infinite order and construct field extensions $L_n = K_n(\frac{1}{\mathfrak{p}^n}Q)$, the field of $\mathfrak{p}^n$-division values of Q. We are able to show that there exists a positive integer e such that L_n/K_n is unramified for $1 \leq n < e$, but L_e/K_e is ramified. Then using properties of formal groups, we are able to compute the conductor of L_e/K_e.

Theorem 1. *There exists a set $\mathfrak{E}$ of at least one and at most g primes of K_e lying over p such that the conductor of L_e/K_e is $\prod_{\mathfrak{P}_e \in \mathfrak{E}} \mathfrak{P}_e^2$.*

If $\mathfrak{E}$ is composed of a lone prime, then we have computed a conductor exactly as in the work of Gupta and of Grant [Gup85, Gra88]. In this case, we will have the same type of congruence relations on units of K_e. If on the other hand $\mathfrak{E}$ is composed of more than one prime, say $\#(\mathfrak{E}) = s > 1$, we have a congruence relation on exterior products of units of K_e.

Theorem 2. *Let $u_1, \ldots, u_s$ be units of K_e, which are congruent to* $1 \bmod \prod_{\mathfrak{P}_e \in \mathfrak{E}} \mathfrak{P}_e$. *Then $u_1 \wedge \cdots \wedge u_s$ is trivial* $\bmod \prod_{\mathfrak{P}_e \in \mathfrak{E}} \mathfrak{P}_e^2$.

This fits more naturally into the framework of Rubin's generalization of Stark's conjecture [Rub96, Sta80]. Stark's conjecture is a generalization of the class number formula, which relates the arithmetic of number fields to special values of Artin L-series. For example, let F/E be a finite abelian extension of number fields and χ a character on $G = \mathrm{Gal}(F/E)$. Let S be a finite set of primes of E including the archimedian primes, the primes which ramify in F, and a set of r primes which split completely in F. Stark's conjecture relates the lead term of the Taylor expansion of the Artin L-series $L(s, \chi)$ at $s = 0$ to the determinant of an $r \times r$ matrix whose entries are linear combinations of logarithms of absolute values of S-units in F (i.e., units locally at all primes not in S). For $r = 1$, Stark gave the following refined conjecture. Let $\mathfrak{P}_1$ be any prime of F sitting over the designated prime of S. Then there exists an S-unit ϵ_1 such that for all characters χ on G

$$L'(0, \chi) = -\frac{1}{w_F} \sum_{\gamma \in G} \chi(\gamma) \log |\gamma(\epsilon_1)|_{\mathfrak{P}_1}.$$

When $F = \mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$, Stark was able to use properties of cyclotomic and elliptic units, respectively, to prove his refined conjecture [Sta80].

For $r \geq 1$, Rubin gave a generalized refined Stark's conjecture, which conjectured a relation between exterior products of S-units and the lead term in the Taylor expansion of $L(s, \chi)$ at $s = 0$ [Rub96]. Rubin's conjecture relates an entry in a lattice of $\mathbb{Q} \otimes \bigwedge^r U_{S,T}$ to the rth derivative at $s = 0$ of $L(s, \chi)$, where $U_{S,T}$ is a specific subgroup of the group of S-units, depending upon an auxiliary, finite set of primes T.

Rubin's conjecture applied to K_e/K should produce exterior products of "abelian S-units" in K_e. Outside of Rubin's original paper, the only direct evidence for Rubin's conjecture is given in [Gra99], which looks at exterior products of units arising from 5-torsion on the Jacobian of $y^2 = x^5 + 1/4$. However, for $g = 1$, Stark further refined his conjecture so that the S-unit in K_n relating to the L-series is actually a unit, and it was congruences on units, not the corresponding S-units, that were employed in the proof of the Coates-Wiles theorem. These results led us to consider whether the existence of a point of infinite order in $A(K)$ should force congruence conditions on *exterior products* of units in K_e; the result of which is Theorem 2.

The first section of this paper fixes notation and assumptions about our abelian variety A and number field K. In the second section, we collect the information we need about formal groups attached to abelian varieties. Then we use properties of formal groups attached to abelian varieties in sections 3 and 4 to describe properties of the field extensions K_n/K and L_n/K_n, respectively. We prove Theorem 1 in section 6 and Theorem 2 in section 7.

Most of the results of this paper were contained in the author's Ph.D. thesis, and the author would be remiss if he did not thank his advisor, David Grant, for his invaluable assistance. Also, the author would like to thank both Wolfgang Schmidt and the Pacific Institute for the Mathematical Sciences for their support during the writing of this paper.

Notation. Let F/E be number fields, and $\mathfrak{q}$ a prime of E. We let $\mathfrak{f}(F/E)$ and $D(F/E)$ denote the conductor and discriminant of F/E respectively. We let $\overline{E}$ denote an algebraic closure of E, $\mathcal{O}_E$ the ring of integers of E, $E_\mathfrak{q}$ the completion of E at $\mathfrak{q}$, and $\mathcal{O}_\mathfrak{q}$ the ring of integers of $E_\mathfrak{q}$.

1. The Setup

We will use the terminology and results of the theory of complex multiplication as developed by Lang in [Lan83] for the results in this section.

Throughout this paper, K will denote a number field of degree $2g$ over $\mathbb{Q}$, which is both Galois and a CM field. Recall that K is a CM field if it is a totally imaginary quadratic extension of a totally real number field. Furthermore we assume that A is an abelian variety of dimension g with complex multiplication by the ring of integers of K. This means that we have an embedding

$$i : K \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q} = \mathrm{End}_{\mathbb{Q}}(A)$$

such that $i(\mathcal{O}_K) = i(K) \cap \mathrm{End}(A)$.

The action of i on the tangent space of A determines a CM type $\Phi = \{\phi_1, \ldots, \phi_g\}$, where ϕ_i, ϕ_j are non-conjugate embeddings of K into $\mathbb{C}$ for $1 \leq i, j \leq g$.

A CM abelian variety will be a pair (A, i). We say that (A, i) is defined over a number field K if both A and every element of $\mathrm{End}(A)$ are defined over K. Let $\overline{K}$ be a fixed algebraic closure of K. For $\alpha \in \mathcal{O}_K$, we put $[\alpha] = i(\alpha) : A(\overline{K}) \to A(\overline{K})$. Therefore we have that $\sigma([\alpha]) = [\sigma(\alpha)]$ for any $\sigma \in \mathrm{Gal}(\overline{K}/K)$. We let $A[\alpha] = \ker[\alpha]$ denote the α-torsion of A.

Throughout this paper p will represent an odd rational prime such that (i) A has good reduction at all primes lying over p and (ii) p splits completely in K. Furthermore we fix a prime $\mathfrak{p}$ of K such that $\mathfrak{p}|p$ and an element $\pi \in \mathcal{O}_K$ such that $\mathrm{ord}_p\pi = \mathrm{ord}_{\mathfrak{p}}\pi = 1$ (such a π exists by the Chinese remainder theorem since p splits completely). For ease of notation, we put $\mathfrak{p}_i = \phi_i(\mathfrak{p})$ for $1 \leq i \leq g$ and let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_g\}$.

Remark. The Jacobians of rational images of Fermat curves are a class of abelian varieties satisfying the assumptions of this section (see [Lan83] or [Shi98] for more details).

2. Formal groups

We need a variety of results on formal groups. We refer to Hazewinkel's excellent book [Haz78] as a general reference on formal groups and to Hindry and Silverman [HS00] for the construction of a formal group attached to an abelian variety and results on the kernel of reduction of A mod $\mathfrak{p}$.

2.1. **Basic Properties.** Let R be a commutative ring with identity and let $X = (X_1, \ldots, X_n)^t$, $Y = (Y_1, \ldots, Y_n)^t$, and $Z = (Z_1, \ldots, Z_n)^t$ be column vectors of variables. We call an n-tuple of power series over R, $F = (F_1, \ldots, F_n)^t$ in $2n$-variables an n-dimensional *commutative formal group (law)* over R if

$$\begin{aligned} F(X, Y) &= X + Y + (d^\circ \geq 2), \\ F(X, F(Y, Z)) &= F(F(X, Y), Z), \text{ and} \\ F(X, Y) &= F(Y, X), \end{aligned}$$

where $(d^\circ \geq m)$ denotes a n-tuple of power series, all of whose terms are of total degree at least m.

If F and G are two n-dimensional formal groups defined over R. A *homomorphism* $\varphi : F \to G$ over R is a n-tuple of power series over R without constant terms such that $\varphi(F(X, Y)) = G(\varphi(X), \varphi(Y))$. A homomorphism is an *isomorphism* if it has a two-sided inverse. Let $\varphi = (\varphi_1, \ldots, \varphi_n)^t$ be a homomorphism from F to G. Suppose that the linear term of $\varphi_i(X_1, \ldots, X_n)^t$ is $\sum_{j=1}^n a_{ij}X_j$. We call the matrix (a_{ij}) the *jacobian* of φ, which we denote by $j(\varphi)$. The following is elementary.

Lemma 2.1. *A homomorphism φ between two n-dimensional formal groups defined over R is an isomorphism if and only if* $\det(j(\varphi))$ *is a unit in R.*

Furthermore, we call two formal groups *strictly isomorphic* over R if there is an isomorphism φ over R such that $j(\varphi)$ is the identity matrix. In [HS00], Hindry and Silverman demonstrate how to construct a g-dimensional commutative formal group $\mathcal{F}$, defined over K, associated to our g-dimensional abelian variety A defined over K. Moreover, $\mathcal{F}$ can be defined over $\mathbb{Z}_p$ and, since p splits completely, we will show that

$\mathcal{F}$ is strictly isomorphic to a product of g one-dimensional formal groups defined over $\mathbb{Z}_p$ of Lubin-Tate type. In order to do this, we need to formalize what we mean by a "product of formal groups".

Let $F = (F_1, \ldots, F_n)^t, G = (G_1, \ldots, G_m)^t$ be n and m-dimensional formal groups, respectively, defined over R. Let $X = (X_1, \ldots, X_n)^t$ and $Y = (Y_1, \ldots, Y_n)^t$ be n-tuples of variables such that $F_i(X, Y) \in R[[X, Y]]$ for $1 \leq i \leq n$. Also let $W = (W_1, \ldots, W_m)^t$ and $Z = (Z_1, \ldots, Z_m)^t$ be m-tuples of variables such that $G_i(W, Z) \in R[[W, Z]]$ for $1 \leq i \leq m$. Then we can define an $(m+n)$-dimensional formal group H over R with $H_i \in R[[X, W, Y, Z]]$ by putting

$$H_i = F_i \text{ for } 1 \leq i \leq n \text{ and}$$
$$H_{n+i} = G_i \text{ for } 1 \leq i \leq m.$$

Specifically, if $\mathcal{G}_1, \ldots, \mathcal{G}_g$ are one-dimensional commutative formal groups over R, then iterating the above construction gives us a g-dimensional commutative formal group over R. Let $\mathcal{G}$ be the formal group constructed in this manner, then we will call such a $\mathcal{G}$ a *product of one-dimensional commutative formal groups*, and write $\mathcal{G} = \oplus_{j=1}^{g} \mathcal{G}_j$. Let φ_j be an endomorphism of $\mathcal{G}_j$ for $1 \leq j \leq g$. Then it is easy to see that $\varphi = (\varphi_1, \ldots, \varphi_g)^t$ is an endomorphism of $\mathcal{G}$, which we will denote by $\varphi = \oplus_{j=1}^{g} \varphi_j$.

2.2. **Properties of the Formal Group $\mathcal{F}$ Associated with A.** Following Hindry and Silverman [HS00], we associate to A a g-dimensional commutative formal group $\mathcal{F}$ over K. Let O denote the origin of A, $\widehat{\mathcal{O}}_A$ the completed local ring at the origin of A, and $\mathfrak{n}$ the maximal ideal of the local ring at the origin of A. Since A is nonsingular, there is an isomorphism $\widehat{\mathcal{O}}_A \cong K[[s_1, \ldots, s_g]]$, where $s_1, \ldots, s_g \in \mathfrak{n}$ are fixed local parameters on A at the origin.

Next we consider the product $A \times A$. Let $p_i : A \times A \to A$ be the projection onto the ith factor for $i = 1, 2$ and for local parameters at the point $(O, O) \in A \times A$ we choose the functions $x_1, \ldots, x_g, y_1, \ldots, y_g$, where $x_i := s_i \circ p_1$ and $y_i := s_i \circ p_2$. Let $\widehat{\mathcal{O}}_{A\times A}$ be the completed local ring at the origin of $A \times A$. Then this choice determines an isomorphism $\widehat{\mathcal{O}}_{A\times A} \cong \widehat{\mathcal{O}}_A \times \widehat{\mathcal{O}}_A \cong k[[x_1, \ldots, x_g, y_1, \ldots, y_g]]$.

The morphism giving the group law on A, $\mathrm{add} : A \times A \to A$, induces a map of local rings $\mathrm{add}^* : \widehat{\mathcal{O}}_A \to \widehat{\mathcal{O}}_{A\times A}$ and by the above isomorphisms, a map $\mathrm{add}^* : k[[s_1, \ldots, s_g]] \to k[[x_1, \ldots, x_g, y_1, \ldots, y_g]]$ of formal power series rings. We let $\mathcal{F}_i = \mathrm{add}^*(s_i)$, and $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_g)^t$. However the formal group $\mathcal{F}$ depends upon the choice of parameters $s_1, \ldots, s_g \in \mathfrak{n}$. Since A is defined over K and the determinant of a change of basis matrix of $\mathfrak{n}/\mathfrak{n}^2$ is a unit in K, Lemma 2.1 shows that all formal groups associated to A in this way are isomorphic over K. Since A has complex multiplication by $\mathcal{O}_K$ and K is Galois over $\mathbb{Q}$, we are able to show that the formal group $\mathcal{F}$ possesses a "CM action".

Lemma 2.2. *There exist local parameters $s_1, \ldots, s_g$ at the origin of A defined over K such that for any $\alpha \in \mathcal{O}_K$*

$$[\alpha]^* s_i := s_i \circ [\alpha] = \phi_i(\alpha) s_i + (d^\circ \geq 2), \text{ in } \widehat{\mathcal{O}}_A. \tag{1}$$

Proof. Let $\mathfrak{P}$ be a prime of K lying over p, then A has good reduction at $\mathfrak{P}$ by assumption. Let $\tilde{A}$ denote the reduced abelian variety mod $\mathfrak{P}$, which is defined over $\tilde{K} = \mathcal{O}_K/\mathfrak{P}\mathcal{O}_K$, and $H^0(A,\Omega)$ the space of holomorphic differentials of A. There exists a basis $\omega_1,\dots,\omega_g$ of differentials defined over K such that $[\alpha]^*\omega_i := \omega_i \circ [\alpha] = \phi_i(\alpha)\omega_i$ for all $1 \le i \le g$ and $\alpha \in \mathcal{O}_K$. Indeed, this follows from [Shi98, pg. 99], since $K/\mathbb{Q}$ is Galois, the field of definition of (A,i) is K, and (A,i) has CM type (K,Φ). We will call such a basis a *splitting basis* for $H^0(A,\Omega)$.

Since $\omega \in H^0(A,\Omega)$ is translation invariant, we can characterize ω by its representation as a differential at the origin [Shi98, pg. 13]. Recall that $\mathfrak{n}$ is the maximal ideal of the local ring at the origin of A, and let ψ be the isomorphism $\mathfrak{n}/\mathfrak{n}^2 \cong H^0(A,\Omega)$ (see [Mil86]), where $\tau \in \mathfrak{n}$ maps to the differential at the origin represented by $d\tau$. Now we pick a $S_i \in \mathfrak{n}$ such that $\psi(S_i) = \omega_i$, and since ψ commutes with endomorphisms of A [Shi98, pg. 75], we have that $[\alpha]^*S_i = \phi_i(\alpha)S_i + (d^\circ \ge 2)$.

We still need to show that we can choose parameters defined over K. Since $\mathrm{Gal}(\overline{K}/K)$ commutes with ψ (see [Shi98]), we see that $\sigma(S_i) = S_i \bmod \mathfrak{n}^2$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. If we let $E = K(S_i)$, then E/K is a finite Galois extension. Now we set $s_i = (1/|\mathrm{Gal}(E/K)|)\sum_{\tau\in\mathrm{Gal}(E/K)}\tau(S_i)$, which gives us the desired parameters, now defined over K. □

By Lemma 2.2, we can define $([\alpha]_{\mathcal{F}})_i(s_1,\dots,s_g) := [\alpha]^*s_i \in K[[s_1,\dots,s_g]]$ for any $\alpha \in \mathcal{O}_K$. Then the map $\alpha \mapsto [\alpha]_{\mathcal{F}} = (([\alpha]_{\mathcal{F}})_1,\dots,([\alpha]_{\mathcal{F}})_g)^t$ gives an embedding of $\mathcal{O}_K$ into the endomorphism ring of $\mathcal{F}$. Next we show that $\mathcal{F}$ and $[\alpha]_{\mathcal{F}}$ are actually defined over $\mathcal{O}_K$.

Lemma 2.3. *There exist local paramaters $s_1,\dots,s_g$ at the origin of A such that $\mathcal{F}$ is defined over $\mathcal{O}_K$ and $[\alpha]_{\mathcal{F}}$ is a g-tuple of power series in $\mathcal{O}_K[[s_1,\dots,s_g]]$ for every $\alpha \in \mathcal{O}_K$. Moreover, if $s = (s_1,\dots,s_g)^t$ then*

$$([\alpha]_{\mathcal{F}}s)_i = \phi_i(\alpha)s_i + (d^\circ \ge 2).$$

Proof. Let $\mathfrak{P}$ be a prime of K lying over p. In the proof of Lemma 2.2, we saw that there exists a splitting basis $\omega_1,\dots,\omega_g$ for $H^0(A,\Omega)$, where the ω_i are defined over K.

For $\omega \in H^0(A,\Omega)$, a suitable multiple of ω will reduce to a non-zero differential on $\tilde{A}$ [Shi98, pg. 80]. When ω reduces to a non-zero differential on $\tilde{A}$, we let $\widetilde{\omega}$ denote the reduced differential. After multiplication by a suitable multiple $a_i \in K$, $\widetilde{a_i\omega_i}$ is non-zero and defined. If we rename $a_i\omega_i$ as ω_i, then the (new) ω_i form a basis for $H^0(A,\Omega)$ such that $[\alpha]^*\omega_i = \phi_i(\alpha)\omega_i$, and hence the CM action is preserved.

Let ψ be the isomorphism between $\mathfrak{n}/\mathfrak{n}^2$ and $H^0(A,\Omega)$ given in the proof of Lemma 2.2 and $s_1,\dots,s_g$ be local parameters at the origin of A over K such that $\psi(s_i) = \omega_i$. Since p is unramified in K by assumption, the $\widetilde{\omega_i}$ form a basis for $H^0(\tilde{A},\Omega)$ [Shi98, pg. 99]. Since ψ commutes with the reduction map mod $\mathfrak{P}$, letting $\widetilde{s_i}$ be the reduction of s_i, the $\widetilde{s_i}$ form a set of parameters at the origin of $\tilde{A}$. Since A has good reduction at $\mathfrak{P}$, the addition map on A reduces to the addition map on $\tilde{A}$. Therefore we can construct a formal group on the reduced abelian variety coming from the parameters $\widetilde{s_1},\dots,\widetilde{s_g}$, which will yield power series $F_i \in (\mathcal{O}_K/\mathfrak{P}\mathcal{O}_K)[[X_1,\dots,X_g,Y_1,\dots,Y_g]]$. By construction,

$\widetilde{add^*s_i} = \widetilde{add^*}\widetilde{s_i}$, so the formal group $\mathcal{F}$ defined by $s_1, \ldots, s_g$ over K reduces mod $\mathfrak{P}$ to $\widetilde{\mathcal{F}_i} = F_i$. Therefore $\mathcal{F}_i \in \mathcal{O}_K[[X_1, \ldots, X_g, Y_1, \ldots, Y_g]]$.

Since endomorphisms of A reduce to endomorphisms of $\tilde{A}$, endomorphisms of $\mathcal{F}$ reduce to endomorphisms of $\tilde{\mathcal{F}}$. Indeed, $\widetilde{[\alpha]^* s_i} = \widetilde{[\alpha]}^* \widetilde{s_i}$ (see [Shi98, pg. 75]), and so we must have $[\alpha]^* s_i \in \mathcal{O}_K[[s_1, \ldots, s_g]]$. □

Remarks.

(1) For a CM elliptic curve, the CM type is usually taken to consist of the identity, so the CM action is trivial.
(2) We will use this CM action to determine which primes ramify. (We became aware of this use of the CM action in [Gra96].)

Let $\Phi'_K = \{\phi_1^{-1}, \ldots, \phi_g^{-1}\}$, then (K, Φ'_K) is a CM type [Lan83, pg. 62]. Let $N_{\Phi'_K}(x) = \prod_{\phi \in \Phi'_K} \phi(x)$ for $x \in K$ and extend $N_{\Phi'_K}$ this to ideals of K in the usual way. Let $\mathfrak{P}$ be a prime of K lying over p, then A has good reduction at $\mathfrak{P}$ by assumption. Since A has principal complex multiplication by K, there exists an element $\alpha_{\mathfrak{P}} \in \mathcal{O}_K$ such that $[\alpha_{\mathfrak{P}}]$ reduces to the Frobenius endomorphism mod $\mathfrak{P}$ (i.e., the endomorphism $x \mapsto x^{N\mathfrak{P}}$ on $\tilde{A}$) [Lan83, pg. 61].

Lemma 2.4. *Let $\mathfrak{P}$ be a prime of K lying over p, and $\alpha_{\mathfrak{P}}$ the element of $\mathcal{O}_K$ which reduces to the Frobenius* mod $\mathfrak{P}$*. Then $\alpha_{\mathfrak{P}}$ has ideal decomposition in K given by*

$$(\alpha_{\mathfrak{P}}) = N_{\Phi'_K}(\mathfrak{P}) = \prod_{j=1}^{g} \phi_j^{-1}(\mathfrak{P}). \tag{2}$$

Moreover, $\mathrm{ord}_{\mathfrak{p}} \alpha_{\mathfrak{P}} = 1$ *if and only if $\mathfrak{P}$ is also in S.*

Proof. The left hand equality in (2) is just [Lan83, pg. 88] and the right hand equality comes from the definition of $N_{\Phi'_K}$. Since p splits completely and $K/\mathbb{Q}$ is Galois, the $\phi_j^{-1}(\mathfrak{P})$ are distinct primes lying over p. On the one hand, if $\mathfrak{P} = \mathfrak{p}_i$ for some $1 \leq i \leq g$, then $\phi_i^{-1}(\phi_i(\mathfrak{p})) = \mathfrak{p}$ is a term in the product. On the other hand, if $\mathfrak{P}|p$, but $\mathfrak{P} \notin S$, then $\mathfrak{p} \neq \phi_j^{-1}(\mathfrak{P})$ for any $1 \leq j \leq g$. □

2.3. **The Kernel of Reduction.** Fix a prime $\mathfrak{P}$ of K lying over p. By base extension, we consider $\mathcal{F}$ defined over $\mathcal{O}_{\mathfrak{P}}$. Let L be a finite extension of $K_{\mathfrak{P}}$, $\mathcal{O}_L$ its ring of integers, and $\mathfrak{m}$ its maximal ideal. By assumption, A considered over $\mathcal{O}_L$ has good reduction at $\mathfrak{m}$, so we let $\tilde{A}$ denotes the reduced abelian variety mod $\mathfrak{m}$, which is defined over $\tilde{L} = \mathcal{O}_L/\mathfrak{m}\mathcal{O}_L$. We define the *kernel of reduction* of A mod $\mathfrak{m}$ by

$$A^\circ(L) := \ker\left\{ A(L) \xrightarrow{red} \tilde{A}(\tilde{L}) \right\}. \tag{3}$$

Now consider $X, Y \in \mathfrak{m}^g = \mathfrak{m} \times \cdots \times \mathfrak{m}$. Then $\mathcal{F}_i(X, Y)$ will converge in $\mathcal{O}_L$. Indeed, $\mathcal{O}_L$ is a complete local ring, and $\mathcal{F}$ is defined over $\mathcal{O}_{\mathfrak{P}} \subseteq \mathcal{O}_L$. Thus the formal group $\mathcal{F}$ defines a group structure on $\mathfrak{m}^g$. Let $\mathcal{F}(\mathfrak{m})$ be the set of g-tuples $\mathfrak{m}^g$ with the group law

$$\mathfrak{m}^g \times \mathfrak{m}^g \xrightarrow{+_{\mathcal{F}}} \mathfrak{m}^g, \text{ given by } \; X +_{\mathcal{F}} Y := \mathcal{F}(X, Y). \tag{4}$$

This gives us the following isomorphism

$$A^\circ(L) \cong \mathcal{F}(\mathfrak{m}), \tag{5}$$

given by $A^\circ(L) \ni R \mapsto (s_1(R), \ldots, s_g(R)) \in \mathfrak{m}^g$ [HS00, Thm. C.2.6].

Now let $\overline{K_\mathfrak{P}}$ be a fixed algebraic closure of $K_\mathfrak{P}$ with valuation ring $\mathcal{O}$ and maximal ideal $\mathcal{M}$. Although $\overline{K_\mathfrak{P}}$ is not complete, each of its elements lives in a finite extension of $K_\mathfrak{P}$. So we extend $+_\mathcal{F}$ to $\mathcal{M}^g$ and identify $\mathcal{F}(\mathcal{M})$ with $A^\circ(\overline{K_\mathfrak{P}})$ (defined analogously to (3)). By Lemma 2.3, $[\alpha]_\mathcal{F}$ is an endomorphism of $\mathcal{F}$ for every $\alpha \in \mathcal{O}_K$. For $\alpha \in \mathcal{O}_K$, we define the *α-torsion of $\mathcal{F}$* to be $\mathcal{F}[\alpha] = \ker\{[\alpha]_\mathcal{F} : \mathcal{F}(\mathcal{M}) \to \mathcal{F}(\mathcal{M})\}$, and for any ideal $\mathfrak{a} \in \mathcal{O}_K$, we define $\mathcal{F}[\mathfrak{a}] = \cap_{\alpha\in\mathfrak{a}}\mathcal{F}[\alpha]$ to be the *$\mathfrak{a}$-torsion* of $\mathcal{F}$.

Lemma 2.5.

(i) *$\mathcal{F}(\mathcal{M})$ has no torsion relatively prime to p.*
(ii) *$A[\mathfrak{p}^n]$ is in the kernel of reduction* mod $\mathcal{M}$ *if and only if $\mathfrak{P} \in S$.*

Proof. (i) This is Proposition C.2.5 of [HS00].

(ii) On the one hand, if $\mathfrak{P} \notin S$ then $[\pi^n]_\mathcal{F}$ is an endomorphism of $\mathcal{F}$. So by Lemma 2.1 the determinant of the jacobian of $[\pi^n]_\mathcal{F}$ is $\det(j([\pi]^n_\mathcal{F})) = \prod_{j=1}^g \phi_j(\pi^n)$. As in the proof of Lemma 2.4, we see that $\mathrm{ord}_\mathfrak{P}\det(j([\pi^n]_\mathcal{F})) = 0$ and therefore $j([\pi^n]_\mathcal{F})$ is invertible. Hence $[\pi^n]_\mathcal{F}$ is an automorphism of $\mathcal{F}(\mathcal{M})$, so $\mathcal{F}(\mathcal{M})$ can have no π^n-torsion. By definition, $\mathcal{F}[\mathfrak{p}^n] \subseteq \mathcal{F}[\pi^n]$, and the result follows.

On the other hand, if $\mathfrak{P} \in S$ and $\alpha_\mathfrak{P}$ is the element of $\mathcal{O}_K$ which reduces to the Frobenius mod $\mathfrak{P}$. Now $[\alpha^n_\mathfrak{P}]$ is a purely inseparable morphism, so $\tilde{A}[\alpha^n_\mathfrak{P}] = \tilde{O}$. Therefore $A[\alpha^n_\mathfrak{P}]$ is in the kernel of reduction mod $\mathfrak{P}$. Basic facts about torsion groups and Lemma 2.4 give that $A[\alpha^n_\mathfrak{P}] = A[\mathfrak{p}^n] \oplus A[\mathfrak{a}]$ for some integral ideal $\mathfrak{a}$ of K. Hence $A[\mathfrak{p}^n]$ is in the kernel of reduction mod $\mathfrak{P}$. □

Corollary 2.6. *Let $\mathfrak{P} \in S$ and consider $\mathcal{F}$ defined over $\mathcal{O}_\mathfrak{P}$. Then we can identify $A[\mathfrak{p}^n]$ with $\mathcal{F}[\pi^n]$.*

Proof. Lemma 2.5 allows us to identify $A[\mathfrak{p}^n]$ with $\mathcal{F}[\mathfrak{p}^n]$, and we know that $\mathcal{F}[\mathfrak{p}^n] \subseteq \mathcal{F}[\pi^n]$. Also, the ideal $\mathfrak{p}^n$ is generated by π^n and $\mathfrak{p}$ for $m > n$. We take m to be a multiple of the class number of K, so that $\mathfrak{p} = (\gamma)$ for some $\gamma \in \mathcal{O}_K$. Then $\pi = \gamma\delta$ with δ relatively prime to p by our choice of π, so $[\delta]$ is an automorphism of $\mathcal{F}$ over $\mathcal{O}_\mathfrak{P}$. Therefore $\mathcal{F}[\mathfrak{p}] = \mathcal{F}[\pi]$, and hence $\mathcal{F}[\mathfrak{p}^n] = \mathcal{F}[\mathfrak{p}] \cap \mathcal{F}[\pi^n] = \mathcal{F}[\pi] \cap \mathcal{F}[\pi^n] = \mathcal{F}[\pi^n]$. □

2.4. **A Product of Formal Groups.** Now we will construct a formal group $\mathcal{G}$ strictly isomorphic to $\mathcal{F}$ over $\mathcal{O}_\mathfrak{P}$ for (fixed) $\mathfrak{P} \in S$, where $\mathcal{G}$ is the product of one-dimensional Lubin-Tate formal groups. This added structure will be very useful in what follows. In order to show that $\mathcal{F}$ is isomorphic to a product of one-dimensional formal groups, we need to recall the properties of higher-dimensional Lubin-Tate formal groups (see [Haz78]).

Remark. In [dS87], de Shalit gave a short proof of this decomposition using the theory of p-divisible groups. However, we need to be careful to show that this isomorphism preserves the CM action as given by Lemma 2.3, and we could not find this anywhere in the literature.

Let $\pi_{\mathfrak{P}}$ be a prime element of $\mathcal{O}_{\mathfrak{P}}$, i.e., $(\pi_{\mathfrak{P}}) = \mathfrak{P}\mathcal{O}_{\mathfrak{P}}$. Let M be a $g \times g$ matrix such that $\pi_{\mathfrak{P}}^{-1}M$ is an invertible matrix with entries in $\mathcal{O}_{\mathfrak{P}}$. We let $\mathcal{E}_M$ denote the set of all g-tuples of power series $d(X)$ in $X = (X_1, \ldots, X_g)^t$ such that

$$d(X) = MX + (d^\circ \geq 2), \quad d(X) \equiv X^p \bmod (\pi_{\mathfrak{P}}). \tag{6}$$

Then the following is [Haz78, Thm. 13.3.3] adapted to our assumptions.

Lemma 2.7. *For each $d(X) \in \mathcal{E}_M$, there is precisely one g-dimensional formal group $F_d(X,Y)$ over $\mathcal{O}_{\mathfrak{P}}$ such that $F_d(d(X), d(Y)) = d(F_d(X,Y))$, so $d \in \mathrm{End}(F_d)$. If $d(X), \overline{d}(X) \in \mathcal{E}_M$, then $F_d(X,Y)$ and $F_{\overline{d}}(X,Y)$ are strictly isomorphic over $\mathcal{O}_{\mathfrak{P}}$.*

For $g = 1$, a formal group satisfying Lemma 2.7 is called a *Lubin-Tate formal group*, and hence is commutative [LT65]. For $g > 1$, we call a formal group F with an endomorphism d as in (6) a *higher dimensional Lubin-Tate formal group*.

For the rest of this section, fix an i with $1 \leq i \leq g$. Then we let $\mathfrak{P} = \phi_i(\mathfrak{p})$, $\alpha_{\mathfrak{P}} \in \mathcal{O}_K$ be such that $[\alpha_{\mathfrak{P}}]$ reduces to the Frobenius mod $\mathfrak{P}$ and $s = (s_1, \ldots, s_g)^t$ represent local parameters over K at the origin of A which are parameters for a g-dimensional commutative formal group $\mathcal{F}$ over $\mathcal{O}_{\mathfrak{P}}$ with CM action as in Lemma 2.3. It will be useful to recall that p splits completely and $\pi \in \mathcal{O}_K$ such that $\mathrm{ord}_{\mathfrak{p}}\pi = \mathrm{ord}_p\pi = 1$.

Lemma 2.8. *$\mathcal{F}$ is a higher dimensional Lubin-Tate formal group defined over $\mathcal{O}_{\mathfrak{P}} \cong \mathbb{Z}_p$.*

Proof. By Lemma 2.3, we have that $[\alpha_{\mathfrak{P}}]^* s_j = \phi_j(\alpha_{\mathfrak{P}})s_j + (d^\circ \geq 2)$. But by Lemma 2.4 $(\alpha_{\mathfrak{P}}) = \prod_{k=1}^g \phi_k^{-1}(\mathfrak{P})$, so $\mathfrak{P}$ exactly divides $\phi_j(\alpha_{\mathfrak{P}})$ for all $1 \leq j \leq g$. Let M be the diagonal matrix whose ith diagonal entry is given by the coefficient of the linear term of $[\alpha_{\mathfrak{P}}]^* s_j$ for each $1 \leq j \leq g$, i.e., $M = \mathrm{diag}\langle \phi_1(\alpha_{\mathfrak{P}}), \ldots, \phi_g(\alpha_{\mathfrak{P}})\rangle$. Let $\pi_{\mathfrak{P}}$ be chosen by the Chinese Remainder Theorem such that $\mathfrak{P}$ exactly divides $(\pi_{\mathfrak{P}})$ and no other conjugate of $\mathfrak{P}$ divides $(\pi_{\mathfrak{P}})$. Then we can write $\phi_j(\alpha_{\mathfrak{P}}) = \pi_{\mathfrak{P}} u_j$ with $u_j \in \mathcal{O}_K$ and u_j relatively prime to $\mathfrak{P}$, and hence $M = \pi_{\mathfrak{P}}\mathrm{diag}\langle u_1, \ldots, u_g\rangle$. The u_j are units in $\mathcal{O}_{\mathfrak{P}}$, so $\pi_{\mathfrak{P}}^{-1}M$ is an invertible matrix. Then we have, by the definition of the Frobenius and since $\mathfrak{P}$ is a first degree prime,

$$[\alpha_{\mathfrak{P}}]_{\mathcal{F}}(s) = Ms + (d^\circ \geq 2), \quad [\alpha_{\mathfrak{P}}]_{\mathcal{F}}(s) \equiv s^p \bmod (\pi_{\mathfrak{P}}).$$

Hence $[\alpha_{\mathfrak{P}}]_{\mathcal{F}} \in \mathcal{E}_M$, and $\mathcal{F}$ is a higher dimensional Lubin-Tate formal group. □

Now we are in a position to decompose $\mathcal{F}$ into a product of one-dimensional formal groups over $\mathfrak{P}$.

Proposition 2.9. *Let everything be as in Lemma 2.8.*

(i) *$\mathcal{F}$ is strictly isomorphic to a product of g one-dimensional commutative formal groups of Lubin-Tate type defined over $\mathcal{O}_{\mathfrak{P}}$, say $\mathcal{G} = \oplus_{j=1}^g \mathcal{G}_j$, where $\mathcal{G}$ is given by paramaters $t = (t_1, \ldots, t_g)^t$.*

(ii) *For each $1 \leq j \leq g$, there is an embedding of $\mathcal{O}_K$ into $\mathrm{End}(\mathcal{G}_j)$ given by $\alpha \mapsto [\alpha]_{\mathcal{G}_j}$, where $[\alpha]_{\mathcal{G}_j} = \alpha t_j + (d^\circ \geq 2)(t_j)$. Then we have an embedding $\mathcal{O}_K$ into $\mathrm{End}(\mathcal{G})$ given by $\alpha \mapsto \oplus_{j=1}^g [\phi_j(\alpha)]_{\mathcal{G}_j}$. Moreover, we can identify $\mathcal{G}[\alpha]$ with $\mathcal{F}[\alpha]$ for all $\alpha \in \mathcal{O}_K$.*

(iii) *Let $\pi_i = \phi_i(\pi)$, then $\mathrm{ord}_{\mathfrak{P}}\pi_i = 1$ and $A[\mathfrak{p}^n]$ can be identified with $\mathcal{G}_i[\pi_i^n]$.*

Proof. (i) Let $M = \mathrm{diag}\langle \phi_1(\alpha_{\mathfrak{P}}), \dots, \phi_g(\alpha_{\mathfrak{P}})\rangle$ and $\pi_{\mathfrak{P}}$ be as in the proof of Lemma 2.8, then $M = \pi_{\mathfrak{P}}\mathrm{diag}\langle u_1, \dots, u_g\rangle$, where $[\alpha_{\mathfrak{P}}]_{\mathcal{F}} s = Ms + (d^\circ \geq 2)$ with $[\alpha_{\mathfrak{P}}]_{\mathcal{F}} \in \mathcal{E}_M$.

Now let $d(t) = (d_1(t_1), \dots, d_g(t_g))^t$, where $d_j(t_j) = \pi_{\mathfrak{P}} u_j t_j + t_j^p$. Then $d(t) \in \mathcal{E}_M$ by construction, and hence, by Lemma 2.7, there exists precisely one g-dimensional formal group F_d over $\mathcal{O}_{\mathfrak{P}}$ such that d is an endomorphism of F_d. We will construct a formal group $\mathcal{G}$, which is a product of one-dimensional Lubin-Tate formal groups, with $d(t)$ an endomorphism of $\mathcal{G}$, and hence, by Lemma 2.7, $\mathcal{G} = F_d$.

Now apply Lemma 2.7 with $M = \pi_{\mathfrak{P}} u_j$ for any $1 \leq j \leq g$. Then $d_j(t_j) \in \mathcal{E}_{\pi_{\mathfrak{P}} u_j}$, so there exists precisely one one-dimensional Lubin-Tate type formal group $\mathcal{G}_j$ over $\mathcal{O}_{\mathfrak{P}}$ such that d_j is an endomorphism of $\mathcal{G}_j$ for each $1 \leq j \leq g$. Let $\mathcal{G} = \oplus_{j=1}^g \mathcal{G}_j$. Therefore $\mathcal{G}$ is a g-dimensional commutative higher dimensional Lubin-Tate formal group. Furthermore, $d(t) = (d_1(t_1), \dots, d_g(t_g))^t$ is an endomorphism of $\mathcal{G}$ by construction, and hence $\mathcal{G} = F_d$. By Lemma 2.7, we have that $\mathcal{F}$ is strictly isomorphic to $\mathcal{G}$ over $\mathcal{O}_{\mathfrak{P}}$.

(ii) For $1 \leq j \leq g$, we know that $\mathcal{G}_j$ is a one-dimensional Lubin-Tate formal group over $\mathcal{O}_{\mathfrak{P}}$ such that $d_j(t_j) = \phi_j(\alpha_{\mathfrak{P}})t_j + t_j^p$ is an endomorphism of $\mathcal{G}_j$. Following [LT65], since $\phi_j(\alpha_{\mathfrak{P}})$ is a uniformizer at $\mathfrak{P}$, we define an endomorphism $[\phi_j(\alpha_{\mathfrak{P}})]_{\mathcal{G}_j}(t_j) := d_j(t_j)$, and for any $\gamma \in \mathcal{O}_{\mathfrak{P}}$, let $[\gamma]_{\mathcal{G}_j}(t_j)$ be the unique power series such that $[\gamma]_{\mathcal{G}_j}(t_j) = \gamma t_j + (d^\circ \geq 2)$ and $[\phi_j(\alpha_{\mathfrak{P}})]_{\mathcal{G}_j}([\gamma]_{\mathcal{G}_j}(t_j)) = [\gamma]_{\mathcal{G}_j}([\phi_j(\alpha_{\mathfrak{P}})]_{\mathcal{G}_j}(t_j))$. Let $m \in \mathbb{Z} \subset \mathcal{O}_{\mathfrak{P}}$, then it is easy to see that multiplication by m coming from the group law on $\mathcal{G}_j$ is an endomorphism of $\mathcal{G}_j$, which must commute with any endomorphism, so is equivalent to the endomorphism $[m]_{\mathcal{G}_j}$ defined by Lubin-Tate theory. Therefore we have an embedding of $\mathbb{Z}[\alpha_{\mathfrak{P}}]$ into $\mathrm{End}(\mathcal{G}_j)$ given by $\beta \mapsto [\phi_j(\beta)]_{\mathcal{G}_j}$ for $\beta \in \mathbb{Z}[\alpha_{\mathfrak{P}}]$, since $\phi_j(m) = m$ for $m \in \mathbb{Z}$. Furthermore, the map $\beta \mapsto \oplus_{j=1}^g [\phi_j(\beta)]_{\mathcal{G}_j}$ gives an embedding of $\mathbb{Z}[\alpha_{\mathfrak{P}}]$ into $\mathrm{End}(\mathcal{G})$. Since $\mathfrak{P}$ is a prime of K of degree one over $\mathbb{Q}$ by assumption, we have that $\mathbb{Z}[\alpha_{\mathfrak{P}}]$ is of finite index in $\mathcal{O}_K$ [Lan83, pg. 88]. Therefore we can extend the above map to an embedding of $\mathcal{O}_K$ into $\mathrm{End}(\mathcal{G})$, where the jacobian of $[\alpha]_{\mathcal{G}} = \mathrm{diag}\langle \phi_1(u), \dots, \phi_g(u)\rangle$.

Now, by (i), there is a strict isomorphism between $\mathcal{F}$ and $\mathcal{G}$, which we denote by β. Therefore $\beta \circ [\alpha]_{\mathcal{F}} \circ \beta^{-1}$ is an endomorphism of $\mathcal{G}$ for all $\alpha \in \mathcal{O}_K$. Since β is a strict isomorphism, $j(\beta) = j(\beta^{-1})$ is the identity matrix, and hence $j(\beta \circ [\alpha]_{\mathcal{F}} \circ \beta^{-1}) = j(\beta) j([\alpha]_{\mathcal{F}}) j(\beta^{-1}) = j([\alpha]_{\mathcal{F}})$. Thus the kernel of $[\alpha]_{\mathcal{F}}$ can be identified with the kernel of $\beta \circ [\alpha]_{\mathcal{F}} \circ \beta^{-1}$. Since these jacobians are equal, Lemma 2.3 shows us that $\beta \circ [\alpha]_{\mathcal{F}} \circ \beta^{-1}(t) = Nt + (d^\circ \geq 2)$, where $N = \mathrm{diag}\langle \phi_1(\alpha), \dots, \phi_g(\alpha)\rangle$. Therefore, for $\alpha \in \mathcal{O}_K$, $[\alpha]_{\mathcal{G}}$ has the same jacobian as $\beta \circ [\alpha]_{\mathcal{F}} \circ \beta^{-1}$, and hence it is easy to see that they have the same kernel. Thus we can identify $\mathcal{F}[\alpha]$ with $\mathcal{G}[\alpha]$ for any $\alpha \in \mathcal{O}_K$.

(iii) By Corollary 2.6, we know that we can identify $A[\mathfrak{p}^n]$ with $\mathcal{F}[\pi^n]$. By construction of the embedding of $\mathcal{O}_K \hookrightarrow \mathrm{End}(\mathcal{G})$ in (ii), we can identify $\mathcal{F}[\pi^n]$ with $\mathcal{G}[\pi^n]$. By definition, we have

$$\begin{aligned}
\mathcal{G}[\pi^n] &= \ker\{[\pi^n]_{\mathcal{G}} : \mathcal{G}(\mathcal{M}) \to \mathcal{G}(\mathcal{M})\} \\
&= \ker\left\{\oplus_{j=1}^g [\phi_j(\pi^n)]_{\mathcal{G}_j} : \oplus_{j=1}^g \mathcal{G}_j(\mathcal{M}) \to \oplus_{j=1}^g \mathcal{G}_j(\mathcal{M})\right\} \\
&= \oplus_{j=1}^g \mathcal{G}_j[\phi_j(\pi^n)] \\
&\cong \mathcal{G}_i[\phi_i(\pi^n)] = \mathcal{G}_i[\pi_i^n].
\end{aligned}$$

Indeed, for $j \neq i$, $\mathrm{ord}_{\mathfrak{P}}\phi_j(\pi^n) = 0$. Therefore $[\phi_j(\pi^n)]_{\mathcal{G}_j}$ is an automorphism, and hence $\mathcal{G}_j[\phi_j(\pi^n)] = \{O\}$. □

Corollary 2.10. *Let everything be as in Proposition 2.9, then*

$$[\pi_i]_{\mathcal{G}_i}(t_i) = \pi_i t_i + u t_i^p + \pi_i \alpha + \beta,$$

where u is unit in $\mathcal{O}_{\mathfrak{P}}$, α and β are power series in t_i with lowest terms of degree two and $2p$ respectively.

Proof. By Proposition 2.9, we know that $[\alpha_{\mathfrak{P}}]_{\mathcal{G}} = \oplus_{j=1}^{g}[\phi_i(\alpha_{\mathfrak{P}})]_{\mathcal{G}_j}$. By Lemma 2.4, we know that $\mathrm{ord}_{\mathfrak{P}}\phi_i(\alpha_{\mathfrak{P}}) = 1$, and hence $\pi_i = \phi_i(\alpha_{\mathfrak{P}})u_i$ with u_i a unit in $\mathcal{O}_{\mathfrak{P}}$. Then we have the following (dropping the $\mathcal{G}_i$ in the notation).

$$\begin{aligned}
[\pi_i](t_i) &= [u_i]([\phi_i(\alpha_{\mathfrak{P}})](t_i)) \\
&= [u_i](\pi_i u_i^{-1} t_i + t_i^p) \\
&= u_i(\pi_i u_i^{-1} t_i + t_i^p) + (d^\circ \geq 2)(\pi_i u_i^{-1} t_i + t_i^p) \\
&= \pi_i t_i + u_i t_i^p + (d^\circ \geq 2)(\pi_i u_i^{-1} t_i + t_i^p).
\end{aligned}$$

□

3. Division fields

In this section, we are interested in algebraic properties of the field extensions of K generated by adjoining $\mathfrak{p}^n$-torsion points to K for K and $\mathfrak{p}$-torsion from A as in section 1. (Recall that this means that $\mathfrak{p}$ is a first-degree prime of K.) We will denote *the field of $\mathfrak{p}^n$-division values of K* by $K_n = K(A[\mathfrak{p}^n])$.

Proposition 3.1. *Let $\mathfrak{P}$ be a prime of K lying over p.*

(i) *K_n/K is totally ramified at $\mathfrak{P} \in S$, and unramified at $\mathfrak{P} \notin S$.*
(ii) *K_n/K is a cyclic extension of degree $p^{n-1}(p-1)$.*
(iii) *Let $\mathfrak{P} = \phi_i(\mathfrak{p})$ for fixed a fixed i with $1 \leq i \leq g$ and let $\mathfrak{P}_n$ be the unique prime of K_n above $\mathfrak{P}$. Then $\mathrm{ord}_{\mathfrak{P}_n} t_i(v) = 1$ for any $v \in A[\mathfrak{p}^n] \setminus A[\mathfrak{p}^{n-1}]$.*

Notation. We denote by S_n the collection of primes $\mathfrak{P}_n$ of K_n described in (iii). By Proposition 5.3 of [Lan83] and (ii), we fix isomorphisms

$$\mathrm{Gal}(K_n/K) \cong (\mathcal{O}_K/\mathfrak{p}^n\mathcal{O}_K)^\times \cong (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

Proof of Proposition 3.1. For now, fix a prime $\mathfrak{P} = \phi_i(\mathfrak{p})$ with $1 \leq i \leq g$. By Proposition 2.9, we can identify $A[\mathfrak{p}^n]$ with $\mathcal{G}_i[\phi_i(\pi^n)]$.

On the one hand, if $\mathfrak{P}_n$ is a prime of K_n lying over $\mathfrak{P}$, we can make the following identification:

$$(K_n)_{\mathfrak{P}_n} = (K(A[\mathfrak{p}^n]))_{\mathfrak{P}_n} = K_{\mathfrak{P}}(A[\mathfrak{p}^n]) = K_{\mathfrak{P}}(\mathcal{G}_i[\phi_i(\pi^n)]).$$

Let $F = K_{\mathfrak{P}}$, and $F_n = K_{\mathfrak{P}}(\mathcal{G}_i[\phi_i(\pi^n)])$. Since $\mathcal{G}_i$ is a Lubin-Tate formal group, F_n/F is a totally ramified cyclic extension of degree $p^{n-1}(p-1)$ (see [LT65]), and hence $[K_n : K] \geq p^{n-1}(p-1)$.

On the other hand, it is well known that $\mathrm{Gal}(K_n/K)$ is isomorphic to a subgroup of $(\mathcal{O}_K/\mathfrak{p}^n\mathcal{O}_K)^\times$. Since p splits completely, we have that $(\mathcal{O}_K/\mathfrak{p}^n\mathcal{O}_K)^\times \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$, where the latter is a cyclic group of order $p^{n-1}(p-1)$. Therefore $[K_n : K] \leq p^{n-1}(p-1)$. This completes the proof of half of (i) and all of (ii).

For (iii), let $\lambda_n = t_i(v)$ for some $v \in A[\mathfrak{p}^n] \setminus A[\mathfrak{p}^{n-1}]$. Since $\mathcal{G}_i$ is a Lubin-Tate formal group, $F_n = F(\lambda_n)$ and $N_{F_n/F}(-\lambda_n) = \phi_i(\pi)$ (see [Neu99, pg. 348]). Note that $(\phi_i(\pi)) = \mathfrak{P}\mathcal{O}_\mathfrak{P}$, and therefore $\mathrm{ord}_{\mathfrak{P}_n}\lambda_n = 1$.

In order to finish (i), let $\mathfrak{P} \notin S$ and $I_{\mathfrak{P}_n}$ be the inertia group of $\mathfrak{P}_n/\mathfrak{P}$. Assume that $\mathfrak{P}$ ramifies in K_n, then $I_{\mathfrak{P}_n} \neq 1$, i.e., there exists a $\sigma \neq 1 \in I_{\mathfrak{P}_n}$ such that $\sigma(\alpha) \equiv \alpha \bmod \mathfrak{P}_n$ for all $\alpha \in \mathcal{O}_{K_n}$. Therefore $\widetilde{\sigma(a)} = \widetilde{a}$ for $a \in A[\mathfrak{p}^n] \setminus A[\mathfrak{p}^{n-1}]$. Since $\sigma \neq 1$, $\sigma(a) - a = b \in A[\mathfrak{p}^n] \setminus \{O\}$. Recall that A has good reduction at all primes above p, therefore the addition map reduces to a morphism on $\tilde{A}$ [HS00, pg. 271]. Hence reduction commutes with addition, and we have that

$$\tilde{O} = \widetilde{\sigma(a)} - \widetilde{a} = \widetilde{\sigma(a) - a} = \tilde{b}.$$

This says that b is in the kernel of reduction, but this contradicts Lemma 2.5. Thus $I_{\mathfrak{P}_n} = 1$, and $\mathfrak{P}$ does not ramify as we claimed. □

Now we are in a position to determine some of the arithmetic properties of the fields K_n/K.

Lemma 3.2. *Let $\mathfrak{P}_1 \in S_1$ and let χ be a non-trivial character on $\mathrm{Gal}(K_n/K_1)$ with $n > 1$. Then $\mathrm{ord}_{\mathfrak{P}_1}\mathfrak{f}(\chi) \geq p$.*

Proof. Let χ be a non-trivial character on the group $\mathrm{Gal}(K_n/K_1)$, which is a cyclic group of order p^{n-1} by Proposition 3.1. For ease of notation, let L_χ denote the fixed field of χ. Then $L_\chi = K_r$ for some $2 \leq r \leq n$, and hence $\mathfrak{f}(\chi) = \mathfrak{f}(K_r/K_1)$ and $\mathfrak{f}(K_2/K_1)|\mathfrak{f}(K_r/K_1)$. Therefore it is enough to show that $\mathfrak{f}((K_2)_{\mathfrak{P}_2}/(K_1)_{\mathfrak{P}_1}) = \mathfrak{P}_1^p$. Once we calculate $D((K_2)_{\mathfrak{P}_2}/(K_1)_{\mathfrak{P}_1})$, the result follows by applying the conductor-discriminant formula (see [Neu99, pg. 534]).

Let $v \in A[\mathfrak{p}^2] \setminus A[\mathfrak{p}]$, then by Proposition 3.1, $t_i(v)$ is a uniformizer at $\mathfrak{P}_2$, and hence $\mathcal{O}_{(K_2)_{\mathfrak{P}_2}} = \mathcal{O}_{(K_1)_{\mathfrak{P}_1}}[t_i(v)]$. Let f be a minimum polynomial for $t_i(v)$, then

$$\begin{aligned} D((K_2)_{\mathfrak{P}_2}/(K_1)_{\mathfrak{P}_1}) &= N_{(K_2)_{\mathfrak{P}_2}/(K_1)_{\mathfrak{P}_1}}(f'(t_i(v)) \\ &= N_{(K_2)_{\mathfrak{P}_2}/(K_1)_{\mathfrak{P}_1}}\Big(\prod_{\substack{u=v+w \\ w\in A[\mathfrak{p}]\setminus\{O\}}} (t_i(v) - t_i(u))\Big) \\ &= \prod_{\substack{u,v\in A[\mathfrak{p}^2]\setminus A[\mathfrak{p}] \\ u\neq v}} (t_i(v) - t_i(u)) \\ &= \mathfrak{P}_1^{p(p-1)}. \end{aligned} \tag{7}$$

Indeed, for each $v \neq u \in A[\mathfrak{p}^2]\setminus A[\mathfrak{p}]$, there exists $w \in A[\mathfrak{p}]\setminus\{O\}$ such that $t_i(v) - t_i(u) = t_i(u+w) - t_i(u) = t_i(w) + (d^\circ \geq 2)(t_i(u), t_i(w))$. By Proposition 3.1, $\mathrm{ord}_{\mathfrak{P}_1}t_i(w) = 1$, and hence by comparing terms of least valuation we have $\mathrm{ord}_{\mathfrak{P}_1}(t_i(v) - t_i(u)) = 1$.

Since $(K_2)_{\mathfrak{P}_2}/(K_1)_{\mathfrak{P}_1}$ is an extension of degree p, the conductor-discriminant formula gives us that $D((K_2)_{\mathfrak{P}_2}/(K_1)_{\mathfrak{P}_1}) = \mathfrak{f}((K_2)_{\mathfrak{P}_2}/(K_1)_{\mathfrak{P}_1})^{p-1}$, and comparing this with (7) completes the result. □

Proposition 3.3. *A has everywhere good reduction over K_1.*

Proof. Since A has complex multiplication by $\mathcal{O}_K$, good reduction at all primes lying over p, and p splits completely in K, the result follows from slight modification to the proof of Theorem 2 of [CW77] (see [Row03] for more details). □

4. The tower

Let h denote the class number of K. Assume that the $\mathcal{O}_K$-rank of $A(K)$ is positive. Let Q be a point of infinite order of A rational over K such that $Q \in A(K) \setminus \mathfrak{p}A(K)$, where $\mathfrak{p}A(K) = \cup_{\alpha\in\mathfrak{p}}[\alpha]A(K)$ (this set is non-empty since the free part of $A(K)$ is a finitely generated $\mathcal{O}_K$-module).

Let $m = rh$ be a positive integer multiple of the class number of K. We have that $\mathfrak{p}^m = (\gamma)$ for some $\gamma \in \mathcal{O}_K$ (hence $A[\mathfrak{p}] = A[\gamma]$). Let $Q_m \in A(\overline{K})$ be such that $[\gamma]Q_m = Q$. We define $L_m = K_m(Q_m)$ to be the field of $\mathfrak{p}$-*division values of* Q which is independent of the choice of Q_m and γ. Then, for $1 \le n \le m$, we define $L_n = K_n(\cup_{\alpha\in\mathfrak{p}^{m-n}}[\alpha]Q_m)$ to be the field of $\mathfrak{p}^n$-*division values of* Q.

Remarks.

(1) Since the class number of K is often not one, we cannot define the field of $\mathfrak{p}^n$-division values of Q in the usual way. Therefore we use the fact that $\mathcal{O}_K$ is a Dedekind domain to note that $\mathfrak{p}^{m-n}$ is generated by two elements of $\mathcal{O}_K$, say $\mathfrak{p}^{m-n} = (\alpha_1, \alpha_2)$. Then it is not hard to see that $L_n = K_n([\alpha_1]Q_m, [\alpha_2]Q_m)$ regardless of the choice of generators for $\mathfrak{p}^{m-n}$.

(2) This definition is independent of our choice of m. Let $m_1 = r_1h$ and $m_2 = r_2h$ with $n < m_1 < m_2$. We can choose Q_{m_2} recursively so that $[\gamma]Q_{r_2h} = Q_{(r_2-1)h}$, and hence $[\gamma^{r_2-r_1}]Q_{m_2} = Q_{m_1}$. Then $\mathfrak{p}^{m_2-n} = \mathfrak{p}^{r_1h-n}\mathfrak{p}^{(r_2-r_1)h} = \mathfrak{p}^{m_1-n}(\gamma^{r_2-r_1})$ and

$$K_n(\cup_{\alpha\in\mathfrak{p}^{m_1-n}}[\alpha]Q_{m_1}) = K_n(\cup_{\alpha\in\mathfrak{p}^{m_1-n}}[\alpha][\gamma^{r_2-r_1}]Q_{m_2}) = K_n(\cup_{\beta\in\mathfrak{p}^{m_2-n}}[\beta]Q_{m_2}).$$

(3) From now on, we may assume that m is a suitably large, fixed multiple of h. Via our isomorphism $\mathcal{O}_K/\mathfrak{p}^n\mathcal{O}_K \cong \mathbb{Z}/p^n\mathbb{Z}$, we indentify $A[\mathfrak{p}^n] \subset A[\mathfrak{p}]$ with the subgroup $\mathfrak{p}^{m-n}\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \subset \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$.

Following [Gup85], we call the fields $L_n \supset K_n \supset K$ the Coates-Wiles tower. It is easy to see that L_n/K is Galois for all n. Furthermore, $G_m = \mathrm{Gal}(L_m/K)$ is identifiable with a subgroup of

$$H_m = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \in GL_2(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K) \right\}.$$

The action of $\sigma = \begin{pmatrix} 1 & a_\sigma \\ 0 & b_\sigma \end{pmatrix} \in G_m$ is given by

$$\sigma(Q_m) = Q_m + a_\sigma,$$
$$\sigma(R) = [b_\sigma]R,$$

where $R, a_\sigma \in A[\mathfrak{p}] \cong \mathcal{O}_K/\mathfrak{p}$ and $b_\sigma \in (\mathcal{O}_K/\mathfrak{p})^\times$.

Since $\mathfrak{p}$ splits completely and we have complex multiplication, we expect the extension L_n/K to be "as big as possible".

Lemma 4.1. $\mathrm{Gal}(L_m/K_m) \cong A[\mathfrak{p}]$.

Proof. We will first show that $L_1 \neq K_1$. Let γ and π be as per usual, so that $\mathfrak{p} = (\gamma)$ and $\mathrm{ord}_\mathfrak{p}\pi = \mathrm{ord}_p\pi = 1$. Then $\mathfrak{p}^{m-1} = (\gamma, \pi^{m-1})$, and we have that $L_1 = K_1([\gamma]Q_m, [\pi^{m-1}]Q_m) = K_1([\pi^{m-1}]Q_m)$. For $\tau \in \mathrm{Gal}(L_1/K)$, we have $\tau([\pi^{m-1}]Q_m) = [\pi^{m-1}]Q_m + a_\tau$ with $a_\tau \in A[\mathfrak{p}] \setminus \{O\}$.

Now assume that $L_1 = K_1$, and define the map $f(\tau) = a_\tau$. It is clear that this defines a 1-cocycle of $\mathrm{Gal}(L_1/K) = \mathrm{Gal}(K_1/K)$ into $A[\mathfrak{p}]$. Since $A[\mathfrak{p}]$ is a p-group, $H^1(\mathrm{Gal}(K_1/K), A[\mathfrak{p}])$ must be a p-group. But Proposition 3.1 shows that $[K_1 : K] = p-1$ and [Ser79, pg. 130] shows that $H^1(\mathrm{Gal}(K_1/K), A[\mathfrak{p}])$ is annihilated by multiplication by $p-1$. Therefore $H^1(\mathrm{Gal}(K_1/K), A[\mathfrak{p}]) = 0$ and f must be a coboundary. Thus there exists $c \in A[\mathfrak{p}]$ such that $f(\tau) = \tau c - c$ for all $\tau \in \mathrm{Gal}(K_1/K)$. Therefore τ fixes $[\pi^{m-1}]Q_m - c$ for all $\tau \in \mathrm{Gal}(K_1/K)$, and hence $[\pi^{m-1}]Q_m - c \in A(K)$. By our choice of π, we must have $\pi = \delta\gamma$ with δ and p relatively prime. But then $[\pi]([\pi^{m-1}]Q_m - c) = [\pi]Q_m = [\delta\gamma]Q_m = [\delta]Q \in A(K)$, which shows that $Q \in [\mathfrak{p}]A(K)$. This is a contradiction of the choice of Q, and hence $L_1 \neq K_1$.

Let $\sigma \in \mathrm{Gal}(L_m/K_m)$. Then it is not hard to see that $\sigma Q_m = Q_m + a_\sigma$ with $a_\sigma \in A[\mathfrak{p}]$ and the map $\sigma \mapsto a_\sigma$ gives us an embedding of $\mathrm{Gal}(L_m/K_m)$ into $A[\mathfrak{p}]$ (for more details see [Row03]). Thus the map $\sigma \mapsto a_\sigma$ injects $\mathrm{Gal}(L_1/K_1)$ into $A[\mathfrak{p}]$. Since L_1/K_1 is non-trivial, $\mathrm{Gal}(L_1/K_1)$ is isomorphic to a non-trivial subgroup of $A[\mathfrak{p}]$. But the only non-trivial subgroup of $A[\mathfrak{p}]$ is $A[\mathfrak{p}]$.

Since $L_1/K_1 \cong A[\mathfrak{p}]$, the rest lemma follows by modifying an argument of Lang for elliptic curves [Lan78]. □

Now we show that, for $n = m$, L_m/K is as big as possible.

Proposition 4.2. $G_m = H_m$.

Proof. By Proposition 3.1, we have that $[K_m : K] = p^{m-1}(p-1)$. By Proposition 5.3 of [Lan83], we have that $A[\mathfrak{p}] \cong \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, and hence $\#(A[\mathfrak{p}]) = p$. By Galois theory and Lemma 4.1, we must have $\#(G_m) = [L_m : K] = pp^{m-1}(p-1)$. By construction $G_m \hookrightarrow H_m$, and a simple calculation shows that $\#(H_m) = pp^{m-1}(p-1) = \#(G_m)$. Therefore $G_m = H_m$. □

Notation. Recall that we fixed an isomorphism such that $A[\mathfrak{p}] \cong \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \cong \mathbb{Z}/p\mathbb{Z}$, where $A[\mathfrak{p}^{m-n}] \subset A[\mathfrak{p}]$ corresponds to $\mathfrak{p}^n\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. For $\alpha \in \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, we say $\alpha \equiv 0 \bmod \mathfrak{p}^n$ if α comes from $A[\mathfrak{p}^{m-n}]$. We will say that $\beta \equiv 1 \bmod \mathfrak{p}^n$ if $\beta \in (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^\times$ acts on $A[\mathfrak{p}^n] \subset A[\mathfrak{p}]$ as the identity automorphism.

Since Proposition 4.2 gives us the matrix representation of $\mathrm{Gal}(L_m/K)$, we can use properties of this matrix group to try and determine the representation of its subgroups.

Proposition 4.3. $\mathrm{Gal}(L_n/K_n) \cong A[\mathfrak{p}^n]$, *and hence* L_n/K *is "as big as possible".*

Proof. It is not hard to see that $L_n \cap K_m = K_n$, and that we have the following isomorphisms:

$$\mathrm{Gal}(L_m/K_n) \cong \left\{ \left(\begin{smallmatrix} 1 & * \\ 0 & \beta \end{smallmatrix}\right) \in \mathrm{GL}_2\left(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K\right) : \beta \equiv 1 \bmod \mathfrak{p}^n \right\} \tag{8}$$

and

$$\mathrm{Gal}(L_m/L_n) \cong \left\{ \left(\begin{smallmatrix} 1 & \alpha \\ 0 & \beta \end{smallmatrix}\right) \in \mathrm{GL}_2\left(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K\right) : \alpha \equiv 0, \beta \equiv 1 \bmod \mathfrak{p}^n \right\}. \tag{9}$$

From equations (8) and (9), we can compute that $[L_m : K_n] = pp^{m-n}$ and $[L_m : L_n] = p^{2m-2n}$. Therefore $[L_n : K_n] = p^{2m-n}/p^{2m-2n} = p^n$.

Since $A[\mathfrak{p}^n]$ is a cyclic group of order p^n and $[L_n : K_n] = p^n$, we need only show that $\mathrm{Gal}(L_n/K_n)$ is isomorphic to a cyclic group. Since $L_n \cap K_m = K_n$, we have $\mathrm{Gal}(L_n/K_n) \cong \mathrm{Gal}(L_nK_m/K_m)$. But the second group is a quotient of the cyclic group $\mathrm{Gal}(L_m/K_m)$, hence it is cyclic. □

In order to compute the conductor of L_n/K_n, we will need to compare calculations made up different branches of the Coates-Wiles tower (see Figure 1). Moreover, we will find the following subextensions of L_n/K helpful in our calculations:

$$M_n := K(\cup_{\alpha \in \mathfrak{p}^{m-n}}[\alpha]Q_m) \tag{10}$$

and

$$\widetilde{M_n} := K_1(\cup_{\alpha \in \mathfrak{p}^{m-n}}[\alpha]Q_m) = K_1M_n \text{ for } 1 \leq n < m. \tag{11}$$

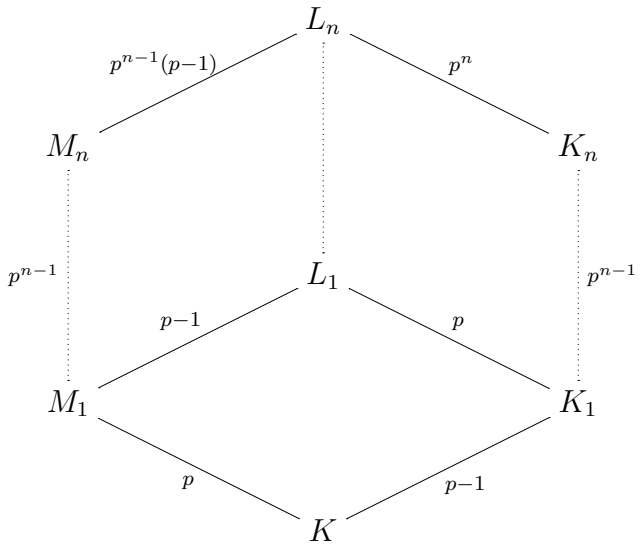

FIGURE 1. The Coates-Wiles tower

5. The Filtration.

We may assume that $Q \in A^\circ(K_\mathfrak{P})$ for all $\mathfrak{P} \in S$, since after multiplying Q by a suitable integer relatively prime to p this is the case. Let $\pi \in \mathcal{O}_K$ such that $\mathrm{ord}_p\pi = \mathrm{ord}_\mathfrak{p}\pi = 1$, and recall that $\mathfrak{p} = (\gamma)$. Then $\pi = \gamma\delta$ with δ and p relatively prime and $\mathfrak{p}^{m-n} = (\gamma, \pi^{m-n})$ for $1 \leq n \leq m$. Thus we have $L_n = K_n([\pi^{m-n}]Q_m)$.

We are interested in computing $\mathfrak{f}(L_n/K_n)$, and the following lemma shows that $\mathfrak{f}(L_n/K_n)$ is only divisible by primes of S_n.

Lemma 5.1. *L_n/K_n is unramified outside of S_n.*

Proof. In Lemma 3.3, we showed that A has everywhere good reduction over K_1, and hence over K_n. It follows easily from Lemma 2.5 that L_n can only be ramified at primes of K_n which lie above p (see [ST68]).

First we will show the result for $n = m$. Let $\mathfrak{q} \notin S_m$ be a prime of K_m above p, $F = (K_m)_\mathfrak{q}$ the completion of K_m at $\mathfrak{q}$, and $A^\circ(F)$ the kernel of reduction mod $\mathfrak{q}$.

Let $\mathfrak{Q}$ be a prime of $\overline{K_m}$ lying over $\mathfrak{q}$, and $I_\mathfrak{Q}$ the inertia group of $\mathfrak{Q}$ over $\mathfrak{q}$. Then $I_\mathfrak{Q}$ acts trivially on Q_m if and only if L_m is unramified at $\mathfrak{q}$. Assume $I_\mathfrak{Q}$ does not act trivially, then there exists $\sigma \neq 1 \in I_\mathfrak{Q}$ such that $\sigma(Q_m)$ and Q_m reduce to the same element mod $\mathfrak{q}$. Therefore $\sigma(Q_m) - Q_m \in A^\circ(F)$, but $\sigma(Q_m) - Q_m = \alpha \in A[\mathfrak{p}]$. Indeed,

$$[\gamma](\sigma(Q_m) - Q_m) = \sigma([\gamma]Q_m) - [\gamma]Q_m = \sigma(Q) - Q = O,$$

where $\mathfrak{p} = (\gamma)$ with $\gamma \in \mathcal{O}_K$. By good reduction at $\mathfrak{q}$, we know that reduction commutes with addition, and hence we have

$$\widetilde{O} = \widetilde{\sigma(Q_m) - Q_m} = \widetilde{\sigma(Q_m)} - \widetilde{Q}_m = \widetilde{\alpha}.$$

By Lemma 2.5, $\alpha = O$, and hence σ acts trivially on Q_m. This contradiction completes the case of $n = m$. For $1 \leq n < m$, let $\mathfrak{q}' \notin S$ be a prime of K lying over p. Then the case of $n = m$ and Proposition 3.1 combine to show us that $\mathfrak{q}$ does not ramify in L_m. Therefore $\mathfrak{q}$ does not ramify in $L_n \subset L_m$, and hence L_n/K_n is unramified outside of S_n. □

For what follows, it is important to recall that

(1) $\mathfrak{P}$ is a prime of K such that $\mathfrak{P} = \phi_i(\mathfrak{p})$ with $1 \leq i \leq g$, where ϕ_i refers to an element of the CM type of A, and
(2) $(\phi_i(\pi)) = (p) = \mathfrak{P}\mathcal{O}_\mathfrak{P}$ locally for some $\pi \in \mathcal{O}_K$.

By Proposition 2.9, we are able to define a filtration of $A^\circ(K_\mathfrak{P})$ for $\mathfrak{P} \in S$. Let $A^\circ(K_\mathfrak{P}) = A_0(K_\mathfrak{P})$ and define

$$A_j(K_\mathfrak{P}) = \{R \in A^\circ(K_\mathfrak{P}) : \mathrm{ord}_\mathfrak{P} t_i(R) > j\}; \tag{12}$$

so $A_0(K_\mathfrak{P}) \supseteq A_1(K_\mathfrak{P}) \supseteq A_2(K_\mathfrak{P}) \supseteq \cdots$

Proposition 5.2. *Let L be a finite extension of K with prime P lying over $\mathfrak{P} \in S$ and let $\beta \in \mathcal{O}_K$ be relatively prime to p. Then*

(i) *$[\pi]_\mathcal{G} : A_j(K_\mathfrak{P}) \to A_{j+1}(K_\mathfrak{P})$ is an isomorphism for all $j \geq 0$.*
(ii) *$[\beta]_\mathcal{G} : A^\circ(L_P) \to A^\circ(L_P)$ is an isomorphism.*

Proof. (i) Proposition 2.9 shows that $\mathcal{G} = \oplus_{k=1}^{g}\mathcal{G}_k$, where $\mathcal{G}_k$ is a one-dimensional Lubin-Tate formal group. What we have done is to construct a filtration on the ith component of this formal group, and by [Ser65] we have an isomorphism on the ith component. Now since $[\pi]_{\mathcal{G}} = \oplus_{k=1}^{g}[\phi_k(\pi)]_{\mathcal{G}_k}$ and $\mathrm{ord}_{\mathfrak{P}}\phi_k(\pi) = 0$ for $k \neq i$, $[\phi_k(\pi)]_{\mathcal{G}_k}$ is an automorphism of $\mathcal{G}_k(\mathfrak{P})$. Indeed, $j([\phi_k(\pi)])$ is a unit in $\mathcal{O}_{\mathfrak{P}}$ for $k \neq i$. Since $A_0(K_{\mathfrak{P}}) \cong \mathcal{G}(\mathfrak{P}) = \oplus_{k=1}^{g}\mathcal{G}_i(\mathfrak{P})$, $[\pi]_{\mathcal{G}}$ is an isomorphism of $A_j(K_{\mathfrak{P}})$ onto $A_{j+1}(K_{\mathfrak{P}})$.

(ii) Given $\beta \in \mathcal{O}_K$ with β and p relatively prime, we have $[\beta]_{\mathcal{G}} = \oplus_{k=1}^{g}[\phi_i(\beta)]_{\mathcal{G}_k}$, and $\phi_k(\beta)$ is a unit in $K_{\mathfrak{P}}$ for all $1 \leq k \leq g$. Then the result follows from a slight modification to the proof of Theorem 3 [Ser65, LG 4.25]. □

Notation. Let $e_{\mathfrak{P}}$ be the smallest integer such that $Q \notin A_{e_{\mathfrak{P}}}(K_{\mathfrak{P}})$, $e = \min_{\mathfrak{P}}\{e_{\mathfrak{P}}\}$, and $\mathfrak{E} = \{\mathfrak{P} \in S : e_{\mathfrak{P}} = e\}$.

Let P_n be a prime of L_n lying over $\mathfrak{P}_n$, for fixed $\mathfrak{P} \in S$. Let $Q = \widetilde{Q}_0$ and choose $\widetilde{Q}_n$ recursively such that $[\pi]\widetilde{Q}_n = \widetilde{Q}_{n-1}$.

Proposition 5.3. *Let P_n be a prime of L_n lying over $\mathfrak{P}_n \in S_n$, then*

$$(L_n)_{P_n} = (K_n)_{\mathfrak{P}_n}(t_i(\widetilde{Q}_n)).$$

Proof. We will first show that $(L_m)_{P_m} = (K_m)_{\mathfrak{P}_m}(\widetilde{Q}_m)$. By definition, we have that $(L_m)_{P_m} = (K_m)_{\mathfrak{P}_m}(Q_m)$. Since $Q \in A^{\circ}(K_{\mathfrak{P}})$ and $[\gamma]Q_m = Q$, there is some choice of $Q_m \in A^{\circ}((L_m)_{P_m})$. Since $A[\mathfrak{p}]$ is in the kernel of reduction, we actually have all choices of $Q_m \in A^{\circ}((L_m)_{P_m})$. By (5), we have that $A^{\circ}((L_m)_{P_m}) \cong \mathcal{G}(P_m)$, where the map is given by $R \mapsto t(R) = (t_1(R), \ldots, t_g(R))^t$. Hence

$$(K_m)_{\mathfrak{P}_m}(Q_m) = (K_m)_{\mathfrak{P}_m}(t_1(Q_m), \ldots, t_g(Q_m))$$

Note that $[\pi]\widetilde{Q}_m = [\gamma]([\delta]\widetilde{Q}_m) = Q$, and hence $[\delta]\widetilde{Q}_m = Q_m + a$ with $a \in A[\mathfrak{p}]$. Therefore, in the formal group, we have that $[\delta]_{\mathcal{G}}t(\widetilde{Q}_m) = t(Q_m + a) = t(Q_m) +_{\mathcal{G}} t(a)$. Since $t(a) \in (K_m)_{P_m}$, we may assume without loss of generality that $a = O$. Since δ is relatively prime to p, Proposition 5.2 gives us that $[\delta]_{\mathcal{G}}$ is an automorphism , and hence invertible. Therefore $[\delta]_{\mathcal{G}}t(\widetilde{Q}_m) = t(Q)$, and we have that

$$(K_m)_{\mathfrak{P}_m}(t_1(Q_m), \ldots, t_g(Q_m)) \subset (K_m)_{\mathfrak{P}_m}(t_1(\widetilde{Q}_m), \ldots, t_g(\widetilde{Q}_m)).$$

The reverse inclusion then comes from $[\delta^{-1}]_{\mathcal{G}}t(Q_m) = t(\widetilde{Q}_m)$. For $1 \leq n < m$, recall that $L_n = K_n([\pi^{m-n}]Q_m)$. As above, we have that

$$(L_n)_{P_n} = (K_n)_{\mathfrak{P}_n}([\pi^{m-n}]Q_m) = (K_n)_{\mathfrak{P}_n}([\pi^{m-n}]\widetilde{Q}_m) = (K_n)_{\mathfrak{P}_n}(\widetilde{Q}_n).$$

Finally, recall that $[\pi^n]_{\mathcal{G}} = \oplus_{k=1}^{g}[\phi_k(\pi^n)]_{\mathcal{G}_k}$, and $[\phi_k(\pi^n)]_{\mathcal{G}_k}$ is an automorphism on $\mathcal{G}_k(\mathfrak{P})$ for $k \neq i$. Hence $t_k(\widetilde{Q}_n) \in \mathcal{G}_k(\mathfrak{P})$ for $k \neq i$, which shows us that

$$(K_n)_{\mathfrak{P}_n}(\widetilde{Q}_n) = (K_n)_{\mathfrak{P}_n}(t_1(\widetilde{Q}_n), \ldots, t_g(\widetilde{Q}_n)) = (K_n)_{\mathfrak{P}_n}(t_i(\widetilde{Q}_n)).$$

□

Notation. Since $(K_n)_{\mathfrak{P}_n}(\widetilde{Q}_n) = (K_n)_{\mathfrak{P}_n}(t_i(\widetilde{Q}_n))$, we will use the notations interchangeably in what follows.

Proposition 5.4. *Let $\mathfrak{P} \in S$ and $e_{\mathfrak{P}}$ be as above. Then*

(i) *for $1 \leq n < e_{\mathfrak{P}}$, $\mathfrak{P}_n$ splits completely in L_n,*
(ii) *$L_{e_{\mathfrak{P}}}/K_{e_{\mathfrak{P}}}$ is ramified over $\mathfrak{P}_{e_{\mathfrak{P}}}$, and*
(iii) *$\mathfrak{P}_{e_{\mathfrak{P}}}$ splits completely in $L_{e_{\mathfrak{P}}-1}K_{e_{\mathfrak{P}}}$. Hence $L_{e_{\mathfrak{P}}}/L_{e_{\mathfrak{P}}-1}K_{e_{\mathfrak{P}}}$ is a totally ramified extension of degree p over any prime above $\mathfrak{P}$.*

Proof. (i) By the filtration (12), we see that there is a $Q_n^{'} \in A_{e_{\mathfrak{P}}-n-1}(K_{\mathfrak{P}})$ such that $[\pi^n]_{\mathcal{G}}t(Q_n^{'}) = t(Q)$. But $[\pi^n]_{\mathcal{G}}t(\widetilde{Q}_n) = t(Q)$, hence $\widetilde{Q}_n = Q_n^{'} + u$ for some $u \in A[\mathfrak{p}^n]$. Since $Q_n^{'} + u \in A((K_n)_{\mathfrak{P}_n})$, we see that $\mathfrak{P}_n$ splits completely. Indeed, there exists a prime P_n of L_n lying over $\mathfrak{P}_n$ such that

$$(L_n)_{P_n} = (K_n)_{\mathfrak{P}_n}(\widetilde{Q}_n) = (K_n)_{\mathfrak{P}_n}(Q_n^{'} + u) = (K_n)_{\mathfrak{P}_n}(u) = (K_n)_{\mathfrak{P}_n}.$$

(ii) Since p splits completely and we have the formal group decomposition of Proposition 2.9, this follows from a slight modification to Theorem 11 of [CW77].

(iii) Let $n = e_{\mathfrak{P}}$. By (i), the decomposition group of $\mathrm{Gal}(L_{n-1}/K_{n-1})$ for $\mathfrak{P}_{n-1}$ is trivial. It is not hard to see that $\mathrm{Gal}(L_{n-1}/K_{n-1}) \cong \mathrm{Gal}(L_{n-1}K_n/K_n)$. Then the decomposition group of $\mathrm{Gal}(L_{n-1}K_n/K_n)$ for $\mathfrak{P}_n$ is isomorphic to a trivial group. Indeed, these decomposition groups are the Galois groups of the corresponding local extensions. Hence $\mathfrak{P}_n$ splits completely in $L_{n-1}K_n$. □

We can reduce the computation of $\mathfrak{f}(L_n/K_n)$ to computing an Artin conductor. If χ is a character of a subgroup H of $\mathrm{Gal}(L_n/K)$, let χ^* be the corresponding induced character on $\mathrm{Gal}(L_n/K)$, and $\mathrm{char}(n) = \{\chi \in \widehat{\mathrm{Gal}}(L_n/K_n) : \chi^{p^{n-1}} \neq 1\}$, where $\widehat{\mathrm{Gal}}(L_n/K_n)$ denotes the character group of $\mathrm{Gal}(L_n/K_n)$. The next lemma demonstrates the importance of computing $\mathfrak{f}(\chi)$ for $\chi \in \mathrm{char}(n)$.

Lemma 5.5. *For any $\chi \in \mathrm{char}(e)$, $\mathfrak{f}(L_e/K_e) = \mathfrak{f}(\chi)$.*

Proof. By definition, $\chi^{p^{e-1}} \neq 1$ for $\chi \in \mathrm{char}(e)$. Hence the fixed field of χ, L_χ, is not contained in K_eL_{e-1}, which is an extension of K_e of degree p^{e-1}. Therefore $L_\chi = L_e$. Since $\mathfrak{f}(\chi) = \mathfrak{f}(L_\chi/K_e)$, we are done. □

6. Conductor Calculations

Let $\mathfrak{E}$ be as in the last section and for the rest of this section fix $\mathfrak{P} \in \mathfrak{E}$. Further, we recall that $\mathfrak{P}_n$ is the unique prime of K_n sitting above $\mathfrak{P}$ in K. By Proposition 5.2 and (10), there exists a prime $\mathcal{P}$ of M_{e-1} over $\mathfrak{P}$ such that

$$(M_{e-1})_{\mathcal{P}} = K_{\mathfrak{P}}.$$

Let $\mathcal{P}_e$ be any prime of $L_{e-1}K_e$ lying over $\mathcal{P}$ and $\mathcal{P}_1$ its restriction to $\widetilde{M}_{e-1}$ (see (11) to recall the definition of $\widetilde{M}_{e-1}$). By (12) and Proposition 5.4, we see that both

$$(L_{e-1}K_e)_{\mathcal{P}_e} = (K_e)_{\mathfrak{P}_e} \text{ and } (\widetilde{M}_{e-1})_{\mathcal{P}_1} = (K_1)_{\mathfrak{P}_1}.$$

Again by Proposition 5.4, there exists a unique totally ramified prime P_e of L_e over $\mathcal{P}_e$ such that $[(L_e)_{P_e} : (L_{e-1}K_e)_{\mathcal{P}_e}] = p$. Let $\wp_1, \wp$ be the restrictions of P_e to $\widetilde{M}_e$ and M_e

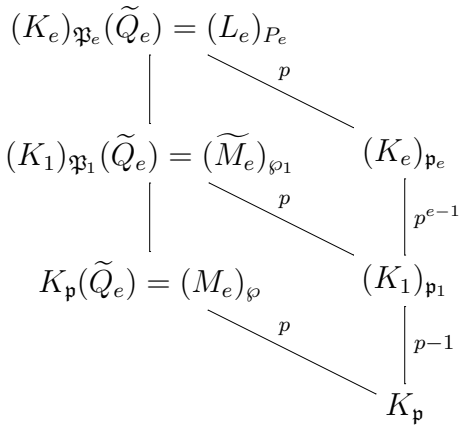

FIGURE 2. The local tower

respectively. The portion of the Coates-Wiles tower we are interested locally is shown in Figure 2, where it is important to note that all of the extensions are totally ramified.

As a first step we will compute the conductor of $(K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1}$, and then use this to compute the conductor of $(K_e)_{\mathfrak{P}_e}(\widetilde{Q}_e)/(K_e)_{\mathfrak{P}_e}$. By Proposition 5.2, we have that $\mathrm{ord}_{\mathfrak{P}} t_i(\widetilde{Q}_{e-1}) = 1$ and $t_i(\widetilde{Q}_{e-1}) = [\pi_i]_{\mathcal{G}_i} t_i(\widetilde{Q}_e)$. In Corollary 2.10, we saw that

$$[\pi_i]_{\mathcal{G}_i}(t_i) = \pi_i t_i + u t_i^p + \pi_i \alpha + \beta,$$

where α, β are power series in t_i with terms of lowest degree two and $2p$ respectively. So

$$t_i(\widetilde{Q}_{e-1}) = [\pi_i]_{\mathcal{G}_i}(t_i)(\widetilde{Q}_e) = \pi_i t_i(\widetilde{Q}_e) + u t_i^p(\widetilde{Q}_e) + \pi_i \alpha(\widetilde{Q}_e) + \beta(\widetilde{Q}_e). \tag{13}$$

Since $(M_e)_{\wp}/K_{\mathfrak{P}}$ is a totally ramified extension of degree p, $\mathrm{ord}_{\wp} t_i(\widetilde{Q}_{e-1}) = p$. Note that $\mathrm{ord}_{\wp} \pi_i t_i(\widetilde{Q}_e) > p$, hence the term on the right-hand side of (13) with least valuation at $\wp$ can only be $u t_i(\widetilde{Q}_e)^p$. Since u is a unit in $\mathcal{O}_{\mathfrak{P}}$, we see that $\mathrm{ord}_{\wp} t_i(\widetilde{Q}_e) = 1$, and we also have $\mathrm{ord}_{\wp_1}(\widetilde{Q}_e) = p-1$ (since $(K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/K_{\mathfrak{P}}(\widetilde{Q}_e)$ is a totally ramified extension of degree $p-1$). Thus $t_i(\widetilde{Q}_e)$ has a $\wp_1$-adic expansion, $\sum_{i \geq p-1} a_i \eta_1^i$, with $a_i \in \{0, \ldots, p-1\}$, $a_{p-1} \neq 0$, and η_1 a uniformizer at $\wp_1$. Indeed, $\mathcal{O}_{\wp_1}/\wp_1 \mathcal{O}_{\wp_1} \cong \mathbb{Z}/p\mathbb{Z}$, so we can take $a_i \in \{0, \ldots, p-1\}$. Therefore we have that

$$(K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1} = (K_1)_{\mathfrak{P}_1}(\eta_1)/(K_1)_{\mathfrak{P}_1}. \tag{14}$$

Let $\sigma \neq \tau \in \mathrm{Gal}((K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1})$, then $\sigma t_i(\widetilde{Q}_e) = t_i(\widetilde{Q}_e + u)$, $\tau t_i(\widetilde{Q}_e) = t_i(\widetilde{Q}_e + v)$ for some $u \neq v \in A[\mathfrak{p}]$. Using the formal group $\mathcal{G}_i$, we see

$$t_i(\widetilde{Q}_e + u) - t_i(\widetilde{Q}_e + v) = t_i(u - v) + (d^\circ \geq 2)(t_i(\widetilde{Q}_e + v), t_i(u - v)). \tag{15}$$

By Proposition 3.1, $t_i(u - v)$ is a uniformizer at $\mathfrak{P}_1$, and hence $\mathrm{ord}_{\wp_1} t_i(u - v) = p$. We also have that $\mathrm{ord}_{\wp_1} t_i(\widetilde{Q}_e + v) = p - 1$, because $\mathrm{ord}_{\wp} t_i(\widetilde{Q}_e + v) = \mathrm{ord}_{\wp} t_i(\widetilde{Q}_e) = 1$ (since any choice of $\widetilde{Q}_e$ will work in (13)). So by comparing the terms of (15) of least valuation

at $\wp_1$ we see that

$$\begin{aligned} p &= \mathrm{ord}_{\wp_1}(t_i(\widetilde{Q}_e + u) - t_i(\widetilde{Q}_e + v)) \\ &= \mathrm{ord}_{\wp_1}(\sum_{i \geq p-1} a_i((\sigma\eta_1)^i - (\tau\eta_1)^i)) \\ &= \mathrm{ord}_{\wp_1}((\sigma\eta_1 - \tau\eta_1)\sum_{i \geq p-1} a_i \sum_{j=0}^{i-1} (\sigma\eta_1)^j(\tau\eta_1)^{i-1-j}) \\ &= \mathrm{ord}_{\wp_1}(\sigma\eta_1 - \tau\eta_1) + \mathrm{ord}_{\wp_1}(\sum_{i \geq p-1} a_i \sum_{j=0}^{i-1} (\sigma\eta_1)^j(\tau\eta_1)^{i-1-j}). \end{aligned} \tag{16}$$

This follows because $x^n - y^n = (x-y)(\sum_{j=0}^{n-1} x^j y^{n-1-j})$. Note that the second term on the last line on the right-hand side of (16) has $\mathrm{ord}_{\wp_1} \geq p-2$. Indeed, $p-2$ is the smallest this valuation can be, since we get at least $p-2$ copies of terms with the same valuation as η_1 in the sum. So (16) implies that

$$\mathrm{ord}_{\wp_1}(\sigma\eta_1 - \tau\eta_1) \leq 2. \tag{17}$$

Now we are in a position to compute the desired conductor.

Proposition 6.1. $\mathfrak{f}((K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1}) = \mathfrak{P}_1^2$

Proof. We know that $(K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1}$ is a totally ramified extension of degree p. Let G represent its Galois group, G_m the mth ramification group of $\wp_1$ over $\mathfrak{P}_1$, and k the exact order of $\mathfrak{P}_1$ dividing $D((K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1})$. Then $k = \sum_{m \geq 0}(\#(G_m) - 1)$. Since $\#(G) = p$ and $\mathfrak{P}_1$ is totally and wildly ramified, we see that $G_0 = G_1 = G$. Therefore $k \geq 2(p-1)$ and $\mathfrak{P}_1^{2(p-1)}$ divides $D((K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1})$.

We know from (14) that η_1 generates $(K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)$. Let f be a minimal polynomial for η_1, and $\sigma, \tau \in G$, then

$$\begin{aligned} D((K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1}) &= N_{(K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1}}(f'(\eta_1)) \\ &= \prod_{\sigma \neq \tau}(\sigma\eta_1 - \tau\eta_1) \,\Big|\, (\wp_1^2)^{p(p-1)} = \mathfrak{P}_1^{2(p-1)}\,. \end{aligned} \tag{18}$$

Comparing equations (18) and (17), we have that $\mathrm{ord}_{\wp_1}(\sigma\eta_1 - \tau\eta_1) = 2$, and hence $D((K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1}) = \mathfrak{P}_1^{2(p-1)}$.

Now let ψ be a non-trivial first degree character on G. Recall that G is cyclic of order p. Therefore there are $p-1$ such characters, and they all have the same conductor, i.e., $\mathfrak{f}(\psi) = \mathfrak{f}((K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1})$. The conductor-discriminant formula and the above calculation yield:

$$\mathfrak{P}_1^{2(p-1)} = D((K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1}) = \mathfrak{f}((K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1})^{p-1}. \tag{19}$$

The result follows on taking $(p-1)$th roots of both sides of (19). □

The following corollary is immediate, and is shown in the proof of the preceding proposition.

Corollary 6.2. *Let ψ be a non-trivial first degree character on the Galois group of $(K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1}$, then $\mathfrak{f}(\psi) = \mathfrak{P}_1^2$.*

Figure 2 begins to illustrate how we will use Proposition 6.1 and Corollary 6.2. The approach is to compute conductors for $n = 1$, and then to use isomorphisms from field theory to lift the results to $n = e$. It is not hard to see that we have the following isomorphism of Galois groups (for more details see [Row03]):

$$\mathrm{Gal}((K_e)_{\mathfrak{P}_e}(\widetilde{Q}_e)/(K_e)_{\mathfrak{P}_e}) \cong \mathrm{Gal}((K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1}), \tag{20}$$

and hence

$$\mathrm{Gal}((K_e)_{\mathfrak{P}_e}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1}) \cong \mathrm{Gal}((K_e)_{\mathfrak{P}_e}(\widetilde{Q}_e)/(K_e)_{\mathfrak{P}_e}) \times \mathrm{Gal}((K_e)_{\mathfrak{P}_e}/(K_1)_{\mathfrak{P}_1}). \tag{21}$$

Proposition 6.3. *Let ψ be any non-trivial first degree character on the Galois group of $((K_e)_{\mathfrak{P}_e}(\widetilde{Q}_e)/(K_e)_{\mathfrak{P}_e})$ and let $\widetilde{\psi}$ be the associated character on the Galois group of $((K_1)_{\mathfrak{P}_1}(\widetilde{Q}_e)/(K_1)_{\mathfrak{P}_1})$ given by* (20)*. Then*

$$\mathrm{ord}_{\mathfrak{P}_e}\mathfrak{f}(\psi) = \mathrm{ord}_{\mathfrak{P}_1}\mathfrak{f}(\widetilde{\psi}).$$

Proof. Given Corollary 6.2 and Lemma 3.2, this follows almost verbatim from the proof of Proposition 5.16 of [Gra88]. □

Proof of Theorem 1. Let χ be a non-trivial first degree character of $\mathrm{Gal}(L_e/K_e)$ such that $\chi^{p^{e-1}} \neq 1$. By Lemma 5.5, we know that $\mathfrak{f}(L_e/K_e) = \mathfrak{f}(\chi)$ and $\mathfrak{f}(\chi)$ is the product of its (local) Artin conductors. Since the only ramification occurs above primes in $\mathfrak{E}$, we need only compute their local conductors. Given the assumption on χ, we see that χ is non-trivial when restricted to $\mathrm{Gal}(L_e/L_{e-1}K_e)$.

And $\mathrm{Gal}(L_e/L_{e-1}K_e) \cong \mathrm{Gal}((K_e)_{\mathfrak{P}_e}(\widetilde{Q}_e)/(K_e)_{\mathfrak{P}_e})$, so we are in a position to apply Proposition 6.3. But Proposition 6.3 combined with Corollary 6.2 gives us the result. □

7. Congruence relations on units

Let e and $\mathfrak{E}$ be as in section 5. Since e is fixed, we will let $F = L_e$, $E = K_e$, and $\mathfrak{P}_i$ represent the unique totally ramified primes of K_e lying over $\mathfrak{p}_i$ of K for $1 \leq i \leq g$. Furthermore, we let $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ be the primes of $\mathfrak{E}$. For an ideal $\mathfrak{m}$ of E, we denote the ray class field modulo $\mathfrak{m}$ by $E(\mathfrak{m})$.

Proposition 7.1. *$E(\mathfrak{P}_1^2 \cdots \mathfrak{P}_s^2)/E(\mathfrak{P}_1\mathfrak{P}_2^2 \cdots \mathfrak{P}_s^2)$ is an extension of degree p.*

Proof. By Theorem 1, we know that the extension $E(\mathfrak{P}_1^2 \cdots \mathfrak{P}_s^2)/E(\mathfrak{P}_1\mathfrak{P}_2^2 \cdots \mathfrak{P}_s^2)$ is non-trivial. Indeed, F/E has conductor $\mathfrak{f}(L/E) = \mathfrak{P}_1^2 \cdots \mathfrak{P}_s^2$, so we must have $E(\mathfrak{P}_1^2 \cdots \mathfrak{P}_s^2) \supseteq F$ and $E(\mathfrak{P}_1\mathfrak{P}_2^2 \cdots \mathfrak{P}_s^2) \not\supseteq F$. Since p is odd and of first degree, the result follows from an easy application of the snake lemma and class field theory. □

Corollary 7.2. *The units of E congruent to* $1 \bmod \mathfrak{P}_1\mathfrak{P}_2^2 \cdots \mathfrak{P}_s^2$ *are also congruent to* $1 \bmod \mathfrak{P}_1^2 \cdots \mathfrak{P}_s^2$.

Remark. Both Gupta and Grant used results similar to Corollary 7.2 to give congruence relations on units. Under our hypotheses, unless $\#(\mathfrak{E}) = 1$, the best we can do is Theorem 2, which gives a congruence relation on an exterior product of units.

Lemma 7.3. *Fix i with $1 \leq i \leq g$ and let v and w be units of E congruent to $1 \bmod \mathfrak{P}_i$. Then there exist relatively prime integers a, b such that $v^a w^b \equiv 1 \bmod \mathfrak{P}_i^2$.*

Proof. By the Chinese remainder theorem, we can choose $\pi \in \mathcal{O}_E$ to be a uniformizer at $\mathfrak{P}_i$. Let v, w have the following $\mathfrak{P}_i$-adic expansions: $v \equiv 1 + \alpha\pi_i \bmod \mathfrak{P}_i^2$ and $w \equiv 1 + \beta\pi_i \bmod \mathfrak{P}_i^2$. Since $N\mathfrak{P}_i = p$, we may choose $\alpha, \beta \in \{0, \ldots, p-1\}$. We see that $v^a w^b \equiv 1 + (\alpha a + \beta b)\pi_i \bmod \mathfrak{P}_i^2$. So by putting $a = \beta/\gcd(\alpha, \beta)$ and $b = -\alpha/\gcd(\alpha, \beta)$, we have $(a, b) = 1$ and $v^a w^b \equiv 1 \bmod \mathfrak{P}_i^2$. □

Lemma 7.4. *Let v, w be units of E such that $v, w \equiv 1 \bmod \mathfrak{P}_i$ and $v^a w^b \equiv 1 \bmod \mathfrak{P}_i^2$ for some relatively prime integers a, b. Then $v \wedge w = v^a w^b \wedge v^c w^d \equiv 1 \wedge v^c w^d \equiv \mathbf{1} \bmod \mathfrak{P}_i^2$, where $c, d \in \mathbb{Z}$ are such that $ad - bc = 1$. That is, $v \wedge w = v' \wedge w'$ with v', w' units such that $v' \equiv 1 \bmod \mathfrak{P}_i^2, w' \equiv 1 \bmod \mathfrak{P}_i$.*

Proof. Since $(a, b) = 1$, there exist integers such that $af + bg = 1$. Let $d = f$ and $c = -g$. By properties of exterior products, $v \wedge w = (ad - bc)(v \wedge w) = v^a w^b \wedge v^c w^d \equiv 1 \wedge v^c w^d \bmod \mathfrak{P}_i^2$. □

With this result, we are now in a position to complete the prooof of the theorem.

Proof of Theorem 2. Note that if $s = 1$ then the result is trivial. We will apply the Lemma 7.4 repeatedly for the primes $\mathfrak{P}_i$ with $2 \leq i \leq s$. Starting with $\mathfrak{P}_2$, we apply Lemma 7.4 as many as $s - 1$ times. Then

$$u_1 \wedge \cdots \wedge u_s = u_1^{'} \wedge \cdots \wedge u_s^{'},$$

where $u_1', \ldots, u_{s-1}' \equiv 1 \bmod \mathfrak{P}_1\mathfrak{P}_2^2\mathfrak{P}_3 \cdots \mathfrak{P}_s$ and $u_s' \equiv 1 \bmod \mathfrak{P}_1 \cdots \mathfrak{P}_s$. So if we do this recursively, we get $u_1 \wedge \cdots \wedge u_s = u_1^{(s-1)} \wedge \cdots \wedge u_s^{(s-1)}$, where

$$\begin{aligned}
u_1^{(s-1)} &\equiv 1 \bmod \mathfrak{P}_1\mathfrak{P}_2^2 \cdots \mathfrak{P}_s^2 \\
u_2^{(s-1)} &\equiv 1 \bmod \mathfrak{P}_1\mathfrak{P}_2^2 \cdots \mathfrak{P}_{s-1}^2\mathfrak{P}_s \\
&\vdots \\
u_{s-1}^{(s-1)} &\equiv 1 \bmod \mathfrak{P}_1\mathfrak{P}_2^2\mathfrak{P}_3 \cdots \mathfrak{P}_s \\
u_s^{(s-1)} &\equiv 1 \bmod \mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_s.
\end{aligned}$$

Now by Corollary 7.2, $u_1^{(s-1)} \equiv 1 \bmod \mathfrak{P}_1^2 \cdots \mathfrak{P}_s^2$. Thus $u_1 \wedge \cdots \wedge u_s \equiv 1 \wedge u_2^{(s-1)} \wedge \cdots \wedge u_s^{(s-1)} \equiv \mathbf{1} \bmod \mathfrak{P}_1^2\mathfrak{P}_2^2 \cdots \mathfrak{P}_s^2$ as desired. □

Corollary 7.5. *Let $u_1, \ldots, u_g$ be units of E congruent to $1 \bmod \mathfrak{P}_1 \cdots \mathfrak{P}_g$, then*

$$u_1 \wedge \cdots \wedge u_g \equiv \mathbf{1} \bmod \mathfrak{P}_1^2 \cdots \mathfrak{P}_g^2.$$

Proof. Let $u_1, \ldots, u_g \equiv 1 \bmod \mathfrak{P}_1 \cdots \mathfrak{P}_g$. By repeated application of Lemma 7.4, we can construct

$$u_1 \wedge \cdots \wedge u_g = \tilde{u}_1 \wedge \cdots \wedge \tilde{u}_g,$$

where $\tilde{u}_1, \ldots, \tilde{u}_s \equiv 1 \bmod \mathfrak{P}_1 \cdots \mathfrak{P}_s\mathfrak{P}_{s+1}^2 \cdots \mathfrak{P}_g^2$. The result follows from applying Theorem 2 to $\tilde{u}_1, \ldots, \tilde{u}_s$. □

References

[CW77] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223–251.

[dS87] E. de Shalit, *On monomial relations between p-adic periods*, J. Reine Angew. Math. **374** (1987), 193–207.

[Gra88] D. Grant, *Coates-Wiles towers in dimension two*, Math. Ann. **282** (1988), 645–666.

[Gra96] ———, *A proof of quintic reciprocity using the arithmetic of* $y^2 = x^5 + 1/4$, Acta Arith. **LXXV** (1996), 321–337.

[Gra99] ———, *Units from 5-torsion on the Jacobian of* $y^2 = x^5 + 1/4$ *and the conjectures of Stark and Rubin*, J. of Number Theory **77** (1999), 227–251.

[Gup85] R. Gupta, *Ramification in the Coates-Wiles tower*, Invent. Math. **81** (1985), 59–69.

[Haz78] M. Hazewinkel, *Formal Groups and Applications*, Academic Press, New York, 1978.

[HS00] M. Hindry and J. H. Silverman, *Diophantine geometry: an introduction*, Springer-Verlag, Berlin/New York, 2000.

[Lan78] S. Lang, *Elliptic Curves: Diophantine Analysis*, Springer-Verlag, Berlin/New York, 1978.

[Lan83] ———, *Complex Multiplication*, Springer-Verlag, Berlin/New York, 1983.

[LT65] J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Ann. of Math.(2) **81** (1965), 380–387.

[Mil86] J.S. Milne, *Abelian varieties*, Arithmetic Geometry (Storrs, Connecticut 1984), Springer-Verlag, Berlin/New York, 1986, pp. 103–150.

[Neu99] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin/Heidelberg, 1999.

[Row03] C. Rowe, *Coates-Wiles Towers for CM-Abelian Varieties*, Ph.D. thesis, University of Colorado at Boulder, 2003.

[Rub87] K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527–560.

[Rub96] ———, *A Stark conjecture "over* $\mathbb{Z}$*" for abelian L-functions with multiple zeros*, Ann. Inst. Fourier **46** (1996), no. 1, 33–62.

[Ser65] J.-P. Serre, *Lie Algebras and Lie Groups*, W.A. Benjamin, New York, 1965.

[Ser79] ———, *Local Fields*, Springer-Verlag, Berlin/New York, 1979.

[Shi98] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, Princeton, New Jersey, 1998.

[ST68] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math.(2) **88** (1968), 492–517.

[Sta80] H. Stark, *L-functions at* $s = 1$*. IV. First derivatives at* $s = 0$, Adv. Math. **35** (1980), 197–235.

[Sta83] ———, *The Coates-Wiles theorem revisited*, Number Theory Related to Fermat's Last Theorem (Progress in Math. Vol. 26), Birkhauser, Boston, 1983, pp. 349–362.

Pacific Institute for the Mathematical Sciences, University of British Columbia, Room 205, 1933 West Mall, Vancouver, BC V6T 1Z2, Canada

E-mail address: rowec@math.ubc.ca